AOS-W 3.3.2 Command Line Interface

Reference Guide

Alcatel·Lucent

Copyright

Trademarks

Legal Notice

Introduction

The AOS-W command line interface (CLI) allows you to configure and manage OmniAccess WLAN switches. The CLI is accessible from a local console connected to the serial port on the WLAN switch or through a Telnet or Secure Shell (SSH) session from a remote management console or workstation.

NOTE: Telnet access is disabled by default on OmniAccess WLAN switches. To enable Telnet access, enter the **telnet cli** command from a serial connection or an SSH session, or in the WebUI navigate to the Configuration > Management > General page.

About this Guide

This guide describes the AOS-W command syntax. The commands in this guide are listed alphabetically.

The following information is provided for each command:

- Command Syntax—The complete syntax of the command.
- Description—A brief description of the command.
- Syntax—A description of the command parameters, including license requirements for specific parameters if needed. The applicable ranges and default values, if any, are also included. The range is a set of values that can be configured. The default can be the default action or state of the WLAN switch.
- Usage Guidelines—Information to help you use the command, including: prerequisites, prohibitions, and related commands.
- Example—An example of how to use the command.
- Platform Availability—The commands described in this guide are available on all platforms, unless otherwise noted.
- Licensing Requirements—The commands described in this guide are available in the base operating system, unless otherwise noted. For more information about available licenses, see the "Managing Software Feature Licenses" chapter in the *AOS-W User Guide*.
- Command Mode—The mode or level within which you use the command. The command can be used on both master and local WLAN switches, unless otherwise noted.

  NOTE: If you can only use the command on the master WLAN switch, all connected local WLAN switches periodically update their configuration. You can manually synchronize all of the WLAN switches at any time by saving the configuration on the master WLAN switch.

- History—The version of AOS-W in which the command was first introduced. Modifications and changes to the command are also noted.

This guide does not include **clear**, **no**, or **show** commands.

Connecting to the WLAN Switch

This section describes how to connect to the WLAN switch to use the CLI.

Serial Port Connection

The serial port is located on the front panel of the WLAN switch. Connect a terminal or PC/workstation running a terminal emulation program to the serial port on the WLAN switch to use the CLI. Configure your terminal or terminal emulation program to use the following communication settings:

Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
9600	8	None	1	None

Telnet or SSH Connection

Telnet or SSH access requires that you configure an IP address and a default gateway on the WLAN switch and connect the WLAN switch to your network. This is typically performed when you run the Initial Setup on the WLAN switch, as described in the *AOS-W Quick Start Guide*. In certain deployments, you can also configure a loopback address for the WLAN switch; see the "Deploying a Basic User-Centric System" chapter in the *AOS-W User Guide* for more information.

CLI Access

When you connect to the WLAN switch using the CLI, the system displays its host name followed by the login prompt. Log in using the admin user account and the password you entered during the Initial Setup on the WLAN switch (the password displays as asterisks). For example:

```
(host)
User: admin
Password: *****
```

When you are logged in, the *user* mode CLI prompt displays. For example:

```
(host) >
```

User mode provides only limited access for basic operational testing such as running **ping** and **traceroute**.

Certain management functions are available in *enable* (also called "privileged") mode. To move from user mode to enable mode requires you to enter an additional password that you entered during the Initial Setup (the password displays as asterisks). For example:

```
(host) > enable
Password: ******
```

When you are in enable mode, the > prompt changes to a pound sign (#):

```
(host) #
```

Configuration commands are available in *config* mode. To move from enable mode to config mode requires that you enter **configure terminal** at the # prompt:

```
(host) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
```

When you are in config mode, (config) appears before the # prompt:

```
(host) (config) #
```

Saving Configuration Changes

Configuration changes made using the CLI affect only the current state of the WLAN switch. Unless saved, the changes are lost when the WLAN switch is rebooted. To save your changes so that they are retained after a reboot, use the following enable mode CLI command:

```
(host) # write memory
Saving Configuration...
Saved Configuration
```

Command Completion

To make command input easier, you can usually abbreviate each key word in the command. You need type only enough of each keyword to distinguish it from similar commands. For example:

```
(host) # configure terminal
```

could also be entered as:

```
(host) # con t
```

Three characters (**con**) represent the shortest abbreviation allowed for **configure**. Typing only **c** or **co** would not work because there are other commands (like **copy**) which also begin with those letters. The configure command is the only one that begins with **con**.

As you type, you can press the spacebar or tab to move to the next keyword. The system then attempts to expand the abbreviation for you. If there is only one command keyword that matches the abbreviation, it is filled in for you automatically. If the abbreviation is too vague (too few characters), the cursor does not advance and you must type more characters or use the help feature to list the matching commands.

Command Help

You can use the question mark (**?**) to view various types of command help.

When typed at the beginning of a line, the question mark lists all the commands available in your current mode or sub-mode. A brief explanation follows each command. For example:

```
(host) > ?

enable            Turn on Privileged commands
logout            Exit this session. Any unsaved changes are lost.
ping              Send ICMP echo packets to a specified IP address.
traceroute        Trace route to specified IP address.
```

When typed at the end of a possible command or abbreviation, the question mark lists the commands that match (if any). For example:

```
(host) > c?

clear                  Clear configuration
clock                  Configure the system clock
configure              Configuration Commands
copy                   Copy Files
```

If more than one item is shown, type more of the keyword characters to distinguish your choice. However, if only one item is listed, the keyword or abbreviation is valid and you can press tab or the spacebar to advance to the next keyword.

When typed in place of a parameter, the question mark lists the available options. For example:

```
(host) # write ?
erase                   Erase and start from scratch
file                    Write to a file in the file system
memory                  Write to memory
terminal                Write to terminal
<cr>
```

The <cr> indicates that the command can be entered without additional parameters. Any other parameters are optional.

Command Line Editing

The command line editing feature allows you to make corrections or changes to a command without retyping. Table 1 lists the editing controls:

TABLE 1 Line Editing Keys

Key	Effect	Description
<Ctrl-a>	Home	Move the cursor to the beginning of the line.
<Ctrl-b> or <left arrow>	Back	Move the cursor one character left.
<Ctrl-d>	Delete Right	Delete the character to the right of the cursor.
<Ctrl-e>	End	Move the cursor to the end of the line.
<Ctrl-f> or <right arrow>	Forward	Move the cursor one character right.
<Ctrl-k>	Kill Right	Delete all characters to the right of the cursor.
<Ctrl-n> or <down arrow>	Next	Display the next command in the command history.
<Ctrl-p> or <up arrow>	Previous	Display the previous command in the command history.
<Ctrl-t>	Transpose	Swap the character to the left of the cursor with the character to the right of the cursor.
<Ctrl-u>	Clear	Clear the line.
<Ctrl-w>	Delete Word	Delete the characters from the cursor up to and including the first space encountered.
<Ctrl-x>	Kill Left	Delete all characters to the left of the cursor.

Alphanumeric characters are always inserted into the line at the cursor position.

Command History

The system records your most recently entered commands. You can review the history of your actions, or reissue a recent command easily, without having to retype it.

To view items in the command history, use the <up arrow> to move back through the list and <down arrow> key to forward. To reissue a specific command, press <enter> when it appears. You can even use the command line editing feature to make changes to the command prior to entering it.

Viewing the Configuration

You can view two configuration images from the CLI:

- startup-config holds the configuration which will be used the next time the WLAN switch is rebooted. It contains all the options last saved using the `write memory` command. Presently unsaved changes are not included.

  To view the startup-config, use the following command:

  ```
  (host) # show startup-config
  ```

- running-config holds the current switch configuration, including all pending changes which have yet to be saved.

  To view the running-config, use the following command:

  ```
  (host) # show running-config
  ```

Both configurations can also be saved to a file or sent to a TFTP server for backup or transfer to another system.

Deleting Configurations

You can use the **no** command to delete or negate previously-entered configurations or parameters.

- To view a list of no commands, type **no** at the enable or config prompt followed by the question mark. For example:

  ```
  (host) (config) # no?
  ```

- To delete a configuration, use the **no** form of a configuration command. For example, the following command removes a configured user role:

  ```
  (host) (config) # no user-role <name>
  ```

- To negate a specific configured parameter, use the **no** parameter within the command. For example, the following commands delete the DSCP priority map for a priority map configuration:

  ```
  (host) (config) # priority-map <name>
  (host) (config-priority-map) # no dscp priority high
  ```

Specifying Network Interfaces in Commands

Any command that references a Fast Ethernet or Gigabit Ethernet interface requires that you specify the corresponding port on the WLAN switch in the format <slot>/<port>, as described in the following:

- <slot> is always 1 except when referring to interfaces on the OmniAccess 6000 WLAN switch (OAW-6000). For the OAW-6000 WLAN switch, the four slots are allocated as follows:
  - Slot 0: contains an OmniAccess Supervisor Card I or II (earlier generation supervisor cards hereinafter referred to as OAW-SC), or OmniAccess Supervisor Card III (OAW-S3).
  - Slot 1: can contain either a redundant OAW-SC, OAW-S3, or a third line card.
  - Slot 2: can contain either an OAW-S3 or line card (required if slot 0 contains an OAW-SC).
  - Slot 3: can contain either an OAW-S3 or second line card.
- <port> refers to the network interfaces that are embedded in the front panel of the OmniAccess 4302 (OAW-4302), 4308 (OAW-4308), 4324 (OAW-4324), 4504 (OAW-4504), 4604 (OAW-4604), and 4704 (OAW-4704) WLAN switches, OAW-S3, or a line card installed in the OAW-6000. Port numbers start at 0 from the left-most position.

Use the **show port status** command to obtain the interface information currently available from a WLAN switch.

Specifying Addresses and Identifiers in Commands

This section describes addresses and other identifiers that you can reference in CLI commands.

TABLE 2 Addresses and Identifiers

Address/Identifier	Description
Network address	For any command that requires entry of an IP address to specify a network entity, use IPv4 network address format in the conventional dotted decimal notation (for example, 10.4.1.258). For subnetwork addresses, specify a netmask in dotted decimal notation (for example, 255.255.255.0).
Media Access Control (MAC) address	For any command that requires entry of a device's hardware address, use the hexadecimal format (for example, 00:05:4e:50:14:aa).
Service Set Identifier (SSID)	A unique character string (sometimes referred to as a network name), consisting of no more than 32 characters. The SSID is case-sensitive (for example, WLAN-01).
Basic Service Set Identifier (BSSID)	This entry is the unique hard-wireless MAC address of the AP. A unique BSSID applies to each frequency— 802.11a and 802.11g—used from the AP. Use the same format as for a MAC address.
Extended Service Set Identifier (ESSID)	Typically the unique logical name of an access point.

Text Conventions

The following conventions are used throughout this manual to emphasize important concepts:

TABLE 3 Text Conventions

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`Commands`	This fixed-width font depicts the following: ■ Command syntax ■ Sample command entry ■ Filenames and commands when mentioned in the text

TABLE 3 Text Conventions (Continued)

`<Arguments>`	In the command syntax, text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: `ping <ipaddr>` In this example, you would type "ping" at the system prompt exactly as shown, followed by the IP address of the system to which ICMP echo packets are to be sent. Do not type the angle brackets.
`[Optional]`	In the command syntax, items enclosed in brackets are optional. Do not type the brackets.
`{Item A|Item B}`	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Contacting Alcatel-Lucent

Contact Center Online	
■ Main Site	http://www.alcatel-lucent.com/enterprise
■ Support Site	https://service.esd.alcatel-lucent.com
■ Email	support@ind.alcatel.com
Service & Support Contact Center Telephone	
■ North America	1-800-995-2696
■ Latin America	1-877-919-9526
■ Europe	+33 (0) 38 855 6929
■ Asia Pacific	+65 6240 8484
■ Worldwide	1-818-878-4507

aaa authentication captive-portal

```
aaa authentication captive-portal <profile>
  clone <source-profile>
  default-role <role>
  enable-welcome-page
  guest-logon
  login-page <url>
  logon-wait {cpu-threshold <percent>|maximum-delay <seconds>|
   minimum-delay <secs>}
  logout-popup-window
  max-authentication-failures <number>
  no ...
  protocol-http
  proxy host <ipaddr> port <port>
  redirect-pause <secs>
  server-group <group-name>
  show-fqdn
  switch-in-redirection-url
  sygate-on-demand-agent
  use-chap
  user-logon
  welcome-page <url>
```

Description

This command configures a Captive Portal authentication profile.

Syntax

Parameter	Description	Range	Default
<profile>	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
clone	Name of an existing Captive Portal profile from which parameter values are copied.	—	—
default-role	Role assigned to the Captive Portal user upon login. When both user and guest logon are enabled, the default role applies to the user logon; users logging in using the guest interface are assigned the guest role.	—	guest
enable-welcome-page	Displays the configured welcome page before the user is redirected to their original URL. If this option is disabled, redirection to the web URL happens immediately after the user logs in.	enabled/ disabled	enabled
guest-logon	Enables Captive Portal logon without authentication.	enabled/ disabled	disabled
login-page	URL of the page that appears for the user logon. This can be set to any URL.	—	/auth/index. html
logon-wait cpu-threshold	CPU utilization percentage above which the Logon wait interval is applied when presenting the user with the logon page.	1-100	60%
logon-wait maximum-delay	Maximum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter.	1-10	10 seconds
logon-wait minimum-delay	Minimum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter.	1-10	5 seconds

Parameter	Description	Range	Default
`logout-popup-window`	Enables a pop-up window with the Logout link for the user to logout after logon. If this is disabled, the user remains logged in until the user timeout period has elapsed or the station reloads.	enabled/ disabled	enabled
`max-authentication-failures`	Maximum number of authentication failures before the user is blacklisted. **NOTE**: The Wireless Intrusion Protection license must be installed.	0-10	0
`no`	Negates any configured parameter.	—	—
`protocol-http`	Use HTTP protocol on redirection to the Captive Portal page. If you use this option, modify the captive portal policy to allow HTTP traffic.	enabled/ disabled	disabled (HTTPS is used)
`proxy`	Configures IP address and port number for proxy server. **NOTE**: This option is only available in the base operating system.	—	N/A
`redirect-pause`	Time, in seconds, that the system remains in the initial welcome page before redirecting the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link.	1-60	10 seconds
`server-group`	Name of the group of servers used to authenticate Captive Portal users. See "aaa server-group" on page 50.	—	—
`show-fqdn`	Allows the user to see and select the fully-qualified domain name (FQDN) on the login page. The FQDNs shown are specified when configuring individual servers for the server group used with captive portal authentication.	enabled/ disabled	disabled
`switch-in-redirection-url`	Sends the WLAN switch's IP address in the redirection URL when external captive portal servers are used. An external captive portal server can determine the WLAN switch from which a request originated by parsing the 'switchip' variable in the URL.	enabled/ disabled	disabled
`sygate-on-demand-agent`	Enables client remediation with Sygate-on-demand-agent (SODA). **NOTE**: The External Services Interface license must be installed.	enabled/ disabled	disabled
`use-chap`	Use CHAP protocol. You should not use this option unless instructed to do so by an Alcatel-Lucent representative.	enabled/ disabled	disabled (PAP is used)
`user-logon`	Enables Captive Portal with authentication of user credentials.	enabled/ disabled	enabled
`welcome-page`	URL of the page that appears after logon and before redirection to the web URL. This can be set to any URL.	—	/auth/welcome.html

Usage Guidelines

You can configure the Captive Portal authentication profile in the base operating system or with the Policy Enforcement Firewall license installed. When you configure the profile in the base operating system, the name of the profile must be entered for the initial role in the AAA profile. Also, when you configure the profile in the base operating system, you cannot define the default-role.

Example

The following example configures a Captive Portal authentication profile that authenticates users against the WLAN switch's internal database. Users who are successfully authenticated are assigned the auth-guest role.

NOTE: To create the auth-guest user role shown in this example, the Policy Enforcement Firewall license must be installed in the WLAN switch.

```
aaa authentication captive-portal guestnet
   default-role auth-guest
   user-logon
   no guest-logon
   server-group internal
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for the noted parameters.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

aaa authentication dot1x

```
aaa authentication dot1x {<profile>|countermeasures}
  ca-cert <certificate>
  clone <profile>
  eapol-logoff
  framed-mtu <mtu>
  heldstate-bypass-counter <number>
  ignore-eap-id-match
  ignore-eapolstart-afterauthentication
  machine-authentication {blacklist-on-failure|cache-timeout <hours>|enable|
   machine-default-role <role>|user-default-role <role>}
  max-authentication-failures <number>
  max-requests <number>
  multicast-keyrotation
  no ...
  opp-key-caching
  reauth-max <number>
  reauthentication
  server {server-retry <number>|server-retry-period <seconds>}
  server-cert <certificate>
  termination {eap-type <type>|enable|enable-token-caching|inner-eap-type
   {eap-gtc|eap-mschapv2}|token-caching-period <hours>}
  timer {idrequest_period <seconds>|mkey-rotation-period <seconds>|
   quiet-period <seconds>|reauth-period <seconds>|server}|
   ukey-rotation-period <seconds>|wpa-groupkey-delay <seconds>|
   wpakey-period <seconds>
  tls-guest-access
  tls-guest-role <role>
  unicast-keyrotation
  use-session-key
  use-static-key
  validate-pmkid
  voice-aware
  wep-key-retries <number>
  wep-key-size {40|128}
  wpa-fast-handover
  wpa-key-retries <number>
  xSec-mtu <mtu>
```

Description

This command configures the 802.1x authentication profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	“default”
`countermeasures`	Scans for message integrity code (MIC) failures in traffic received from clients. If there are more than 2 MIC failures within 60 seconds, the AP is shut down for 60 seconds. This option is intended to slow down an attacker who is making a large number of forgery attempts in a short time.	—	disabled
`ca-cert`	CA certificate for client authentication. The CA certificate needs to be loaded in the WLAN switch.	—	—
`clone`	Name of an existing 802.1x profile from which parameter values are copied.	—	—
`eapol-logoff`	Enables handling of EAPOL-LOGOFF messages.	—	disabled

Parameter	Description	Range	Default
framed-mtu	Sets the framed MTU attribute sent to the authentication server.	500-1500	1100
heldstate-by pass-counter	(This parameter is applicable when 802.1x authentication is terminated on the WLAN switch, also known as AAA FastConnect.) Number of consecutive authentication failures which, when reached, causes the WLAN switch to not respond to authentication requests from a client while the WLAN switch is in a held state after the authentication failure. Until this number is reached, the WLAN switch responds to authentication requests from the client even while the WLAN switch is in its held state.	0-3	0
ignore-eap-id-match	Ignore EAP ID during negotiation.	—	disabled
ignore-eapol start-afterauthentication	Ignores EAPOL-START messages after authentication.	—	disabled
machine-authentication	(For Windows environments only) These parameters set machine authentication: **NOTE**: The Policy Enforcement Firewall license must be installed.		
enable	Select this option to enforce machine authentication before user authentication. If selected, either the machine-default-role or the user-default-role is assigned to the user, depending on which authentication is successful.	—	disabled
blacklist-on-failure	Blacklists the client if machine authentication fails.	—	disabled
cache-timeout	The timeout, in hours, for machine authentication.	1-1000	24 hours (1 day)
machine-default-role	Default role assigned to the user after completing only machine authentication.	—	guest
user-default-role	Default role assigned to the user after 802.1x authentication.	—	guest
max-authentication-failures	Number of times a user can try to login with wrong credentials after which the user is blacklisted as a security threat. Set to 0 to disable blacklisting, otherwise enter a non-zero integer to blacklist the user after the specified number of failures. **NOTE**: The Wireless Intrusion Protection license must be installed.	0-5	0 (disabled)
max-requests	Maximum number of times ID requests are sent to the client.	1-10	3
multicast-key rotation	Enables multicast key rotation	—	disabled
no	Negates any configured parameter.	—	—
opp-key-caching	Enables a cached pairwise master key (PMK) derived with a client and an associated AP to be used when the client roams to a new AP. This allows clients faster roaming without a full 802.1x authentication. **NOTE**: Make sure that the wireless client (the 802.1x supplicant) supports this feature. If the client does not support this feature, the client will attempt to renegotiate the key whenever it roams to a new AP. As a result, the key cached on the WLAN switch can be out of sync with the key used by the client.	—	enabled

Parameter	Description	Range	Default
reauth-max	Maximum number of times ID requests are sent to the client.	1-10	3
reauthentication	Select this option to force the client to do a 802.1x reauthentication after the expiration of the default timer for reauthentication. (The default value of the timer is 24 hours.) If the user fails to reauthenticate with valid credentials, the state of the user is cleared. If derivation rules are used to classify 802.1x-authenticated users, then the reauthentication timer per role overrides this setting.	—	disabled
server	Sets options for sending authentication requests to the authentication server group.		
server-retry	Maximum number of authentication requests that are sent to server group.	0-3	2
server-retry-period	Server group retry interval, in seconds.	5-65535	30 seconds
server-cert	Server certificate used by the WLAN switch to authenticate itself to the client.	—	—
termination	Sets options for terminating 802.1x authentication on the WLAN switch.		
enable	Enables 802.1x termination on the WLAN switch.	—	disabled
eap-type	The Extensible Authentication Protocol (EAP) method, either EAP-PEAP or EAP-TLS.	eap-peap/ eap-tls	eap-peap
enable-token-caching	If you select EAP-GTC as the inner EAP method, you can enable the WLAN switch to cache the username and password of each authenticated user. The WLAN switch continues to reauthenticate users with the remote authentication server, however, if the authentication server is not available, the WLAN switch will inspect its cached credentials to reauthenticate users.	—	disabled
inner-eap-type	When EAP-PEAP is the EAP method, one of the following inner EAP types is used: ■ EAP-Generic Token Card (GTC): Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the WLAN switch as a backup to an external authentication server. ■ EAP-Microsoft Challenge Authentication Protocol version 2 (MS-CHAPv2): Described in RFC 2759, this EAP method is widely supported by Microsoft clients.	eap-gtc/eap-mschapv2	eap-mschap v2
token-caching-period	If you select EAP-GTC as the inner EAP method, you can specify the timeout period, in hours, for the cached information.	(any)	24 hours
timer	Sets timer options for 802.1x authentication:		
idrequest_period	Interval, in seconds, between identity request retries.	1-65535	30 seconds
mkey-rotation-period	Interval, in seconds, between multicast key rotation.	60-864000	1800 seconds
quiet-period	Interval, in seconds, following failed authentication.	1-65535	30 seconds

Parameter	Description	Range	Default
reauth-period	Interval, in seconds, between reauthentication attempts, or specify **server** to use the server-provided reauthentication period.	60-864000	86400 seconds (1 day)
ukey-rotation-period	Interval, in seconds, between unicast key rotation.	60-864000	900 seconds
wpa-groupkey-delay	Interval, in seconds, between unicast and multicast key exchanges.	0-2000	0 seconds (no delay)
wpakey-period	Interval, in seconds, between each WPA key exchange.	1-5	3 seconds
tls-guest-access	Enables guest access for EAP-TLS users with valid certificates.	—	disabled
tls-guest-role	User role assigned to EAP-TLS guest. **NOTE**: The Policy Enforcement Firewall license must be installed.	—	guest
unicast-keyrotation	Enables unicast key rotation.	—	disabled
use-session-key	Use RADIUS session key as the unicast WEP key.	—	disabled
use-static-key	Use static key as the unicast/multicast WEP key.	—	disabled
validate-pmkid	When **opp-key-caching** is enabled, this option instructs the WLAN switch to check the pairwise master key (PMK) ID sent by the client. When this option is enabled, the client must send a PMKID in the associate or reassociate frame to indicate that it supports OKC; otherwise, full 802.1x authentication takes place. (This feature is optional, since most clients that support OKC do not send the PMKID in their association request.)	—	disabled
voice-aware	Enables rekey and reauthentication for VoWLAN clients. **NOTE**: The Voice Services Module license must be installed.	—	enabled
wep-key-retries	Number of times unicast/multicast EAPOL key messages are sent to the client.	1-3	2
wep-key-size	Dynamic WEP key size, either 40 or 128 bits.	40 or 128	128 bits
wpa-fast-handover	Enables WPA-fast-handover. This is only applicable for phones that support WPA and fast handover.	—	disabled
wpa-key-retries	Number of times WPA/WPA2 key messages are retried.	1-5	3
xSec-mtu	Sets the size of the MTU for xSec.	1024-1500	1300 bytes

Usage Guidelines

The 802.1x authentication profile allows you to enable and configure machine authentication and 802.1x termination on the WLAN switch (also called “AAA FastConnect”).

In the AAA profile, you specify the 802.1x authentication profile, the default role for authenticated users, and the server group for the authentication.

Example

The following example enables authentication of the user's client device before user authentication. If machine authentication fails but user authentication succeeds, the user is assigned the restricted "guest" role:

```
aaa authentication dot1x dot1x
   machine-authentication enable
   machine-authentication machine-default-role computer
   machine-authentication user-default-role guest
```

The following example configures an 802.1x profile that terminates authentication on the WLAN switch, where the user authentication is performed with the WLAN switch's internal database or to a "backend" non-802.1x server:

```
aaa authentication dot1x dot1x
   termination enable
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system. The voice-aware parameter requires the Voice Services Module license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

aaa authentication mac

```
aaa authentication mac <profile>
  case upper|lower
  clone <profile>
  delimiter {colon|dash|none}
  max-authentication-failures <number>
  no ...
```

Description

This command configures the MAC authentication profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
`case`	The case (upper or lower) used in the MAC string sent in the authentication request. If there is no delimiter configured, the MAC address in lower case is sent in the format xxxxxxxxxxxx, while the MAC address in upper case is sent in the format XXXXXXXXXXXX.	upperllower	lower
`clone`	Name of an existing MAC profile from which parameter values are copied.	—	—
`delimiter`	Delimiter (colon, dash, or none) used in the MAC string.	colonldashl none	none
`max-authentication-failures`	Number of times a client can fail to authenticate before it is blacklisted. A value of 0 disables blacklisting.	0-10	0 (disabled)
`no`	Negates any configured parameter.	—	—

Usage Guidelines

MAC authentication profile configures authentication of devices based on their physical MAC address. MAC-based authentication is often used to authenticate and allow network access through certain devices while denying access to all other devices. Users may be required to authenticate themselves using other methods, depending upon the network privileges.

Example

The following example configures a MAC authentication profile to blacklist client devices that fail to authenticate.

```
aaa authentication mac mac-blacklist
  max-authentication-failures 3
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

Beginning with AOS-W 3.3.1.8, the max-authentication-failures parameter was allowed in the base operating system. In earlier versions of AOS-W, the max-authentication-failures parameter required the Wireless Intrusion Protection license.

aaa authentication mgmt

```
aaa authentication mgmt
   default-role
    {guest-provisioning|location-api|network-operations|no-access|read-only|root}
   enable
   no ...
   server-group <group>
```

Description

This command configures authentication for administrative users.

Syntax

Parameter	Description	Range	Default
`default-role`	A predefined management role assigned to authenticated administrative users.	—	guest
`enable`	Enables authentication for administrative users.	enabledl disabled	disabled
`no`	Negates any configured parameter.	—	—
`server-group`	Name of the group of servers used to authenticate administrative users. See "aaa server-group" on page 50.	—	default

Usage Guidelines

If you enable authentication with this command, users configured with the **mgmt-user** command must be authenticated using the specified server-group.

You can configure the management authentication profile in the base operating system or with the Policy Enforcement Firewall license installed.

Example

The following example configures a management authentication profile that authenticates users against the WLAN switch's internal database. Users who are successfully authenticated are assigned the read-only role.

```
aaa authentication mgmt
   default-role read-only
   server-group internal
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

The network-operations role was introduced in AOS-W 3.2.

The location-api-mgmt role was introduced in AOS-W 3.3.

aaa authentication stateful-dot1x

```
aaa authentication stateful-dot1x
  default-role <role>
  enable
  no ...
  server-group <group>
  timeout <seconds>
```

Description

This command configures 802.1x authentication for clients on non-OmniAccess APs.

Syntax

Parameter	Description	Range	Default
`default-role`	Role assigned to the 802.1x user upon login. **NOTE**: The Policy Enforcement Firewall license must be installed.	—	guest
`enable`	Enables 802.1x authentication for clients on non-OmniAccess APs. Use **no enable** to disable this authentication.	—	enabled
`no`	Negates any configured parameter.	—	—
`server-group`	Name of the group of RADIUS servers used to authenticate the 802.1x users. See "aaa server-group" on page 50.	—	—
`timeout`	Timeout period, in seconds.	1-20	10 seconds

Usage Guidelines

This command configures 802.1x authentication for clients on non-OmniAccess APs. The WLAN switch maintains user session state information for these clients.

Example

The following command assigns the employee user role to clients who successfully authenticate with the server group corp-rad:

```
aaa authentication stateful-dot1x
  default-role employee
  server-group corp-rad
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for the noted parameter.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

aaa authentication stateful-dot1x clear

```
aaa authentication stateful-dot1x clear
```

Description

This command clears automatically-created control path entries for 802.1x users on non-OmniAccess APs.

Syntax

No parameters.

Usage Guidelines

Run this command after changing the configuration of a RADIUS server in the server group configured with the **aaa authentication stateful-dot1x** command. This causes entries for the users to be created in the control path with the updated configuration information.

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

aaa authentication vpn

```
aaa authentication vpn
  default-role <role>
  max-authentication-failures <number>
  no ...
  server-group <group>
```

Description

This command configures VPN authentication.

Syntax

Parameter	Description	Range	Default
`default-role`	Role assigned to the VPN user upon login. **NOTE**: The Policy Enforcement Firewall license must be installed.	—	guest
`max-authentication-failures`	Maximum number of authentication failures before the user is blacklisted. A value of 0 disables blacklisting. **NOTE**: The Wireless Intrusion Protection license must be installed.		0 ((disabled)
`no`	Negates any configured parameter.	—	—
`server-group`	Name of the group of servers used to authenticate VPN users. See "aaa server-group" on page 50.	—	internal

Usage Guidelines

This command configures VPN authentication settings. Use the **vpdn group** command to enable and configure Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPSec) or Point-to-Point Tunneling Protocol (PPTP) VPN connection. (See "vpdn group l2tp" on page 362 or "vpdn group pptp" on page 364.)

Example

The following command configures VPN authentication settings:

```
aaa authentication vpn
  default-role employee-role-vpn
  max-authentication-failures 0
  server-group vpn-server-group
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for the noted parameters.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa authentication wired

```
aaa authentication wired
  no ...
  profile <aaa-profile>
```

Description

This command configures authentication for a client device that is directly connected to a port on the WLAN switch.

Syntax

Parameter	Description	Range	Default
`no`	Negates any configured parameter.	—	—
`profile`	Name of the AAA profile that applies to wired authentication. This profile must be configured for a Layer-2 authentication, either 802.1x or MAC. See "aaa profile" on page 45.	—	

Usage Guidelines

This command references an AAA profile that is configured for MAC or 802.1x authentication. The port on the WLAN switch to which the device is connected must be configured as untrusted.

Example

The following commands configure an AAA profile for dot1x authentication and a wired profile that references the AAA profile:

```
aaa profile sec-wired
  dot1x-default-role employee
  dot1x-server-group sec-svrs
aaa authentication wired
  profile sec-wired
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa authentication-server internal

```
aaa authentication-server internal use-local-switch
```

Description

This command specifies that the internal database on a local WLAN switch be used for authenticating clients.

Syntax

Parameter	Description	Range	Default
`use-local-switch`	Specifies that the local WLAN switch's internal database is used.	—	database on master is used

Usage Guidelines

By default, the internal database in the *master* WLAN switch is used for authentication. This command directs authentication to the internal database on the *local* WLAN switch where you run the command.

Platform Availability

This command is available on all platforms.

NOTE: You run this command on a local WLAN switch.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

aaa authentication-server ldap

```
aaa authentication-server ldap <server>
   admin-dn <name>
   admin-passwd <string>
   allow-cleartext
   authport <port>
   base-dn <name>
   clone <server>
   enable
   filter
   host <ipaddr>
   key-attribute <string>
   no ...
   timeout <seconds>
```

Description

This command configures an LDAP server.

Syntax

Parameter	Description	Range	Default
`ldap`	Name that identifies the server.	—	—
`admin-dn`	Distinguished name for the admin user who has read/search privileges across all of the entries in the LDAP database (the user does not need write privileges but should be able to search the database and read attributes of other users in the database).	—	—
`admin-passwd`	Password for the admin user.	—	—
`allow-cleartext`	Allows clear-text (unencrypted) communication with the LDAP server.	enabledl disabled	disabled
`authport`	Port number used for authentication. Port 636 will be attempted for LDAP over SSL, while port 389 will be attempted for SSL over LDAP, Start TLS operation and clear text.	1-65535	389
`base-dn`	Distinguished Name of the node which contains the entire user database to use.	—	—
`clone`	Name of an existing LDAP server configuration from which parameter values are copied.	—	—
`enable`	Enables the LDAP server.	—	
`filter`	Filter that should be applied to search of the user in the LDAP database (default filter string is: ì(objectclass=*)î).	—	(objectclass=) *
`host`	IP address of the LDAP server.	—	—
`key-attribute`	Attribute that should be used as a key in search for the LDAP server. For Active Directory, the value is sAMAccountName.	—	sAMAccou ntName
`no`	Negates any configured parameter.	—	—
`timeout`	Timeout period of a LDAP request, in seconds.	1-30	20 seconds

Usage Guidelines

You configure a server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see “aaa server-group” on page 50).

Example

The following command configures and enables an LDAP server:

```
aaa authentication-server ldap ldap1
   host 10.1.1.243
   base-dn cn=Users,dc=1m,dc=corp,dc=com
   admin-dn cn=corp,cn=Users,dc=1m,dc=corp,dc=com
   admin-passwd abc10
   key-attribute sAMAccountName
   filter (objectclass=*)
   enable
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa authentication-server radius

```
aaa authentication-server radius <server>
  acctport <port>
  authport <port>
  clone <server
  enable
  host <ipaddr>
  key <psk>
  nas-identifier <string>
  nas-ip <ipaddr>
  no ...
  retransmit <number>
  timeout <seconds>
  use-md5
```

Description

This command configures a RADIUS server.

Syntax

Parameter	Description	Range	Default
`radius`	Name that identifies the server.	—	—
`acctport`	Accounting port on the server.	1-65535	1813
`authport`	Authentication port on the server	1-65535	1812
`clone`	Name of an existing RADIUS server configuration from which parameter values are copied.	—	—
`enable`	Enables the RADIUS server.		
`host`	IP address of the RADIUS server.	—	—
`key`	Shared secret between the WLAN switch and the authentication server. The maximum length is 48 bytes.	—	—
`nas-identifier`	Network Access Server (NAS) identifier to use in RADIUS packets.	—	—
`nas-ip`	NAS IP address to send in RADIUS packets. You can configure a "global" NAS IP address that the WLAN switch uses for communications with all RADIUS servers. If you do not configure a server-specific NAS IP, the global NAS IP is used. To set the global NAS IP, enter the **ip radius nas-ip** *ipaddr* command.	—	—
`no`	Negates any configured parameter.	—	—
`retransmit`	Maximum number of retries sent to the server by the WLAN switch before the server is marked as down.	0-3	3
`timeout`	Maximum time, in seconds, that the WLAN switch waits before timing out the request and resending it.	1-30	5 seconds
`use-md5`	Use MD5 hash of cleartext password.	—	disabled

Usage Guidelines

You configure a server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see "aaa server-group" on page 50).

Example

The following command configures and enables a RADIUS server:

```
aaa authentication-server radius radius1
   host 10.1.1.244
   key qwERtyuIOp
   enable
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa authentication-server tacacs

```
aaa authentication-server tacacs <server>
  clone <server>
  enable
  host <ipaddr>
  key <psk>
  no ...
  retransmit <number>
  tcp-port <port>
  timeout <seconds>
```

Description

This command configures a TACACS+ server.

Syntax

Parameter	Description	Range	Default
`tacacs`	Name that identifies the server.	—	—
`clone`	Name of an existing TACACS server configuration from which parameter values are copied.	—	—
`enable`	Enables the TACACS server.	—	
`host`	IP address of the TACACS server.	—	—
`key`	Shared secret to authenticate communication between the TACACS+ client and server.	—	—
`no`	Negates any configured parameter.	—	—
`retransmit`	Maximum number of times a request is retried.	0-3	3
`tcp-port`	TCP port used by the server.	1-65535	49
`timeout`	Timeout period of a TACACS request, in seconds.	1-30	20 seconds

Usage Guidelines

You configure a server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see “aaa server-group” on page 50).

Example

The following command configures and enables a TACACS+ server:

```
aaa authentication-server tacacs tacacs1
  clone default
  host 10.1.1.245
  key qwERtyuIOp
  enable
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa bandwidth-contract

```
aaa bandwidth-contract <name> {kbits <kbits>|mbits <mbits>}
```

Description

This command configures a bandwidth contract.

Syntax

Parameter	Description	Range	Default
`<name>`	Name that identifies this bandwidth contract.	—	—
`kbits`	Number of kilobits per second.	256-2000000	—
`mbits`	Number of megabits per second.	1-2000	—

Usage Guidelines

You can apply a configured bandwidth contract to a user role or to a VLAN. When you apply a bandwidth contract to a user role (see "user-role" on page 357), you specify whether the contract applies to upstream traffic (from the client to the WLAN switch) or downstream traffic (from the WLAN switch to the client). You can also specify whether the contract applies to all users in a specified user role or per-user in a user role.

When you apply a bandwidth contract to a VLAN (see "interface vlan" on page 206), the contract limits multicast traffic and does not affect other data. This is useful because an AP can only send multicast traffic at the rate of the slowest associated client. Thus excessive multicast traffic will fill the buffers of the AP, causing frame loss and poor voice quality. Generally, every system should have a bandwidth contract of 1 Mbps or even 700 Kbps and it should be applied to all VLANs with which users are associated, especially those VLANs that pass through the upstream router. The exception are VLANs that are used for high speed multicasts, where the SSID is configured without low data rates.

Example

The following command creates a bandwidth contract that limits the traffic rate to 1 Mbps:

```
aaa bandwidth-contract mbits 1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

The Policy Enforcement Firewall license must be installed.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa derivation-rules

```
aaa derivation-rules user <name>
  no ...
  set {role|vlan} condition <rule-type> <condition> <value> set-value {<role>|<vlan>}
   [position <number>]
```

Description

This command configures rules by which the role or VLAN assigned to a client is derived from the client's association with an AP.

NOTE: The Policy Enforcement Firewall must be installed for a user role to be assigned.

Syntax

Parameter	Description	Range	Default
`user`	Name that identifies this set of user derivation rules.	—	—
`no`	Negates a configured rule.	—	—
`condition`	Rule type, condition, and value that determine if the value of set-value is applied to the client. Each rule type allows specific conditions and values, as described in the following:	—	—

`bssid`	BSSID of AP to which client is associated. The condition must be one of the following:
	`contains`
	`ends with`
	`equals`
	`does not equal`
	`starts with`
	The value must be a full or partial MAC address (xx:xx:xx:xx:xx:xx format).
		—	—

`dhcp-option-77`	User class identifier (option 77) returned by DHCP server. The condition must be: `equals` The value must be a string.	—	—

`encryption-type`	Encryption type used by the client. The condition must be one of the following:
	`equals`
	`does not equal`
	The value can be one of the following:
	`dynamic-aes`
	`dynamic-tkip`
	`dynamic-wep`
	`open`
	`static-aes`
	`static-tkip`
	`static-wep`
	`xsec`
		—	—

`essid`	ESSID to which the client is associated. The condition must be one of the following:
	`contains`
	`ends with`
	`equals`
	`does not equal`
	`starts with`
	`value of`
	For all conditions except value-of, the value must be a string. For the value-of condition, you do not configure the set-value parameter; the ESSID is used to set the VLAN or user role.
		—	—

`location`	AP name or AP group which includes the AP to which the client is associated. The condition must be one of the following:
	`equals`
	`does not equal`
	The value must be a string.
		—	—

`macaddr`	MAC address of the client. The condition must be one of the following:
	`contains`
	`ends with`
	`equals`
	`does not equal`
	`starts with`
	The value must be a full or partial MAC address (xx:xx:xx:xx:xx:xx format).
		—	—

`set-value`	Sets the user role or VLAN ID to be assigned to the client if the condition is met.	—	—
`position`	Position of this rule relative to other rules configured for this set of rules.		1

Usage Guidelines

The user role can be derived from attributes from the client's association with an AP. You configure the user role to be derived by specifying condition rules; when a condition is met, the specified user role is assigned to the client. You can specify more than one condition rule; the order of rules is important as the first matching condition is applied.

NOTE: User-derivation rules are executed *before* the client is authenticated.

Example

The following command sets the client's user role to "guest" if the client associates to the "Guest" ESSID.

```
aaa derivation-rules user derive1
  set role condition essid equals Guest set-value guest
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system. The Policy Enforcement Firewall must be installed for a user role to be assigned.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

aaa inservice

```
aaa inservice <server-group> <server>
```

Description

This command designates an “out of service” authentication server to be “in service”.

Syntax

Parameter	Description	Range	Default
<server-group>	Server group to which this server is assigned.	—	—
<server>	Name of the configured authentication server.	—	—

Usage Guidelines

By default, the WLAN switch marks an unresponsive authentication server as “out of service” for a period of 10 minutes (you can set a different time limit with the **aaa timers dead-time** command). The **aaa inservice** command is useful when you become aware that an “out of service” authentication server is again available before the dead-time period has elapsed. (You can use the **aaa test-server** command to test the availability and response of a configured authentication server.)

Example

The following command sets an authentication server to be in service:

```
aaa inservice corp-rad rad1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode.

History

This command was available in AOS-W 3.0.

aaa ipv6 user add

```
aaa ipv6 user add <ipv6addr> [authentication-method
{dot1x|mac|stateful-dot1x|vpn|web}][mac <macaddr>] [name <username>]
[profile <aaa_profile>] [role <role>]
```

Description

This command manually assigns a user role or other values to a specified IPv6 client.

Syntax

Parameter	Description	Range	Default
`<ipv6addr>`	IPv6 address of the user to be added.	—	—
`authentication-method`	Authentication method for the user.	—	—
`dot1x`	802.1x authentication.		
`stateful-dot1x`	Stateful 802.1x authentication.		
`mac`	MAC address of the user.	—	—
`name`	Name for the user.	—	—
`profile`	AAA profile for the user.	—	—
`role`	Role for the user.	—	—

Usage Guidelines

This command should only be used for troubleshooting issues with a specific IPv6 client. This command allows you to manually assign a client to a role. For example, you can create a role “debugging” that includes a policy to mirror session packets to a specified destination for further examination, then use this command to assign the “debugging” role to a specific client. Use the **aaa ipv6 user delete** command to remove the client or device from the role.

Note that issuing this command does not affect ongoing sessions that the client may already have. For example, if a client is in the “employee” role when you assign them to the “debugging” role, the client continues any sessions allowed with the “employee” role. Use the **aaa ipv6 user clear-sessions** command to clear ongoing sessions.

Example

The following commands create a role that logs HTTPS traffic, then assign the role to a specific IPv6 client:

```
ipv6 access-list session ipv6-log-https
   any any svc-https permit log
user-role ipv6-web-debug
   session-acl ipv6-log-https
```

In enable mode:

```
aaa ipv6 user add 2002:d81f:f9f0:1000:e409:9331:1d27:ef44 role ipv6-web-debug
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was introduced in AOS-W 3.3.

aaa ipv6 user clear-sessions

```
aaa ipv6 user clear-sessions <ipaddr>
```

Description

This command clears ongoing sessions for the specified IPv6 client.

Syntax

Parameter	Description	Range	Default
`clear-sessions`	IPv6 address of the user.	—	—

Usage Guidelines

This command clears any ongoing sessions that the client already had before being assigned a role with the **aaa ipv6 user add** command.

Example

The following command clears ongoing sessions for an IPv6 client:

```
aaa user clear-sessions 2002:d81f:f9f0:1000:e409:9331:1d27:ef44
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was introduced in AOS-W 3.3.

aaa ipv6 user delete

```
aaa ipv6 user delete {<ipaddr>|all|mac <macaddr>|name <username>|role <role>}
```

Description

This command deletes IPv6 clients, users, or roles.

Syntax

Parameter	Description	Range	Default
`<ipv6addr>`	IPv6 address of the client to be deleted.	—	—
`all`	Deletes all connected IPv6 clients.	—	—
`mac`	MAC address of the IPv6 client to be deleted.	—	—
`name`	Name of the IPv6 client to be deleted.	—	—
`role`	Role of the IPv6 client to be deleted.	—	—

Usage Guidelines

This command allows you to manually delete clients, users, or roles. For example, if you used to the **aaa ipv6 user add** command to assign a user role to an IPv6 client, you can use this command to remove the role assignment.

Example

The following command a role:

```
aaa ipv6 user delete role web-debug
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was introduced in AOS-W 3.3.

aaa ipv6 user logout

```
aaa ipv6 user logout <ipaddr>
```

Description

This command logs out an IPv6 client.

Syntax

Parameter	Description	Range	Default
<ipv6addr>	IPv6 address of the client to be logged out.	—	—

Usage Guidelines

This command logs out an authenticated IPv6 client. The client must reauthenticate.

Example

The following command logs out an IPv6 client:

```
aaa user logout 2002:d81f:f9f0:1000:e409:9331:1d27:ef44
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was introduced in AOS-W 3.3.

aaa profile

```
aaa profile <profile>
  authentication-dot1x <dot1x-profile>
  authentication-mac <mac-profile>
  clone <profile>
  dot1x-default-role <role>
  dot1x-server-group <group>
  initial-role <role>
  mac-default-role <role>
  mac-server-group <group>
  no ...
  radius-accounting <group>
  rfc-3576-server <ipaddr>
  sip-authentication-role <role>
  user-derivation-rules <profile>
  wired-to-wireless-roam
  xml-api-server <ipaddr>
```

Description

This command configures the authentication for a WLAN.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies this instance of the profile. The name must be 1-63 characters.	—	"default"
`authentication-dot1x`	Name of the 802.1x authentication profile associated with the WLAN. See "aaa authentication dot1x" on page 13.	—	—
`authentication-mac`	Name of the MAC authentication profile associated with the WLAN. See "aaa authentication mac" on page 18.	—	—
`clone`	Name of an existing AAA profile configuration from which parameter values are copied.	—	—
`dot1x-default-role`	Configured role assigned to the client after 802.1x authentication. If derivation rules are present, the role assigned to the client through these rules take precedence over the default role. **NOTE**: The Policy Enforcement Firewall license must be installed.	—	guest
`dot1x-server-group`	Name of the server group used for 802.1x authentication. See "aaa server-group" on page 50.	—	—
`initial-role`	Role for unauthenticated users.	—	logon
`mac-default-role`	Configured role assigned to the user when the device is MAC authenticated. If derivation rules are present, the role assigned to the client through these rules take precedence over the default role. **NOTE**: The Policy Enforcement Firewall license must be installed.	—	guest
`mac-server-group`	Name of the server group used for MAC authentication. See "aaa server-group" on page 50.	—	—
`no`	Negates any configured parameter.	—	—
`radius-accounting`	Name of the server group used for RADIUS accounting. See "aaa server-group" on page 50.	—	—

rfc-3576-server	IP address of a RADIUS server that can send user disconnect and change-of-authorization messages, as described in RFC 3576, "Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS)". See "aaa rfc-3576-server" on page 49. **NOTE**: The External Services Interface license must be installed.	—	—
sip-authentication-role	Configured role assigned to a session initiation protocol (SIP) client upon registration. **NOTE**: The Voice Services Module license must be installed.	—	guest
user-derivation-rules	User attribute conditions from which the user role or VLAN is derived.	—	—
wire-to-wireless-roam	Keeps user authenticated when roaming from the wired side of the network.	—	enabled
xml-api-server	IP address of a configured XML API server. See "aaa xml-api" on page 65. **NOTE**: The External Services Interface license must be installed.	—	—

Usage Guidelines

The AAA profile defines the user role for unauthenticated users, the default user role for MAC or 802.1x authentication, and user derivation rules. The AAA profile contains the authentication profile and authentication server group.

There are predefined AAA profiles available: default-dot1x, default-mac-auth, and default-open, that have the parameter values shown in Table 4.

TABLE 4 Parameter Values for Predefined AAA Profile

Parameter	default-dot1x	default-mac-auth	default-open
authentication-dot1x	default	N/A	N/A
authentication-mac	N/A	default	N/A
dot1x-default-role	authenticated	guest	guest
dot1x-server-group	N/A	N/A	N/A
initial-role	logon	logon	logon
mac-default-role	guest	authenticated	guest
mac-server-group	default	default	default
radius-accounting	N/A	N/A	N/A
rfc-3576-server	N/A	N/A	N/A
user-derivation-rules	N/A	N/A	N/A
wired-to-wireless roam	enabled	enabled	enabled

Example

The following command configures an AAA profile that assigns the “employee” role to clients after they are authenticated using the 802.1x server group “radiusnet”.

```
aaa profile corpnet
   dot1x-default-role employee
   dot1x-server-group radiusnet
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for the noted parameters.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

aaa radius-attributes

```
aaa radius-attributes add <attribute> <attribute-id> {date|integer|ipaddr|string}
[vendor <name> <vendor-id>]
```

Description

This command configures RADIUS attributes for use with server derivation rules.

Syntax

Parameter	Description	Range	Default
`add`	Adds the specified attribute name (alphanumeric string), associated ID (integer), and type (date, integer, IP address, or string).	—	—
`vendor`	Optional vendor name and vendor ID.	—	—

Usage Guidelines

Add RADIUS attributes for use in server derivation rules. Use the **show aaa radius-attributes** command to display a list of the current RADIUS attributes recognized by the WLAN switch. To add a RADIUS attribute to the list, use the **aaa radius-attributes** command.

Example

The following command adds the VSA “Alcatel-Lucent-User-Role”:

```
aaa radius-attributes add Alcatel-Lucent-User-Role 1 string vendor Aruba 14823
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa rfc-3576-server

```
aaa rfc-3576-server <ipaddr>
  clone <server>
  key <psk>
  no ...
```

Description

This command configures a RADIUS server that can send user disconnect and change-of-authorization messages, as described in RFC 3576, “Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS)”.

Syntax

Parameter	Description	Range	Default
`<ipaddr>`	IP address of the server.	—	—
`clone`	Name of an existing RFC 3576 server configuration from which parameter values are copied.	—	—
`key`	Shared secret to authenticate communication between the RADIUS client and server.	—	—
`no`	Negates any configured parameter.	—	—

Usage Guidelines

The server configured with this command is referenced in the AAA profile for the WLAN (see “aaa profile” on page 45).

Example

The following command configures an RFC 3576 server:

```
aaa rfc-3576-server 10.1.1.245
  clone default
  key asdfjkl;
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

The External Services Interface license must be installed.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

aaa server-group

```
aaa server-group <group>
  allow-fail-through
  auth-server <name> [{match-authstring {contains|equals|starts-with} <string> |
   match-fqdn <string>}][position <number>][trim-fqdn]
  clone <group>
  no ...
  set {role|vlan} condition <attribute>
   {{contains|ends-with|equals|not-equals|starts-with} <string> set-value
   {<role>|<vlan>}|value-of} [position <number>]
```

Description

This command allows you to add a configured authentication server to an ordered list in a server group, and configure server rules to derive a user role or VLAN from attributes returned by the server during authentication.

Syntax

Parameter	Description	Range	Default
`<group>`	Name that identifies the server group. The name must be 32 characters or less.	—	—
`allow-fail-through`	When this option is configured, an authentication failure with the first server in the group causes the WLAN switch to attempt authentication with the next server in the list. The WLAN switch attempts authentication with each server in the ordered list until either there is a successful authentication or the list of servers in the group is exhausted.	—	disabled
`auth-server`	Name of a configured authentication server.	—	—
`match-auth string`	This option associates the authentication server with a match rule that the WLAN switch can compare with the user/client information in the authentication request. With this option, the user/client information in the authentication request can be in any of the following formats: ■ <domain>\<user> ■ <user>@<domain> ■ host/<pc-name>.<domain> An authentication request is sent to the server only if there is a match between the specified match rule and the user/client information. You can specify the following match conditions: ■ contains: The rule matches if the user/client information contains the specified string. ■ equals: The rule matches if the user/client information exactly matches the specified string. ■ starts-with: The rule matches if the user/client information starts with a specified string. You can configure multiple match rules for an authentication server.	—	—

`match-fqdn`	This option associates the authentication server with a specified domain. An authentication request is sent to the server only if there is an exact match between the specified domain and the <domain> portion of the user information sent in the authentication request. With this option, the user information must be in one of the following formats: ■ <domain>\<user> ■ <user>@<domain>	—	—
`position`	Position of the server in the server list. 1 is the top.	—	(last)
`trim-fqdn`	This option causes the user information in an authentication request to be edited before the request is sent to the server. Specifically, this option: ■ removes the <domain>\ portion for user information in the <domain>\<user> format ■ removes the @<domain> portion for user information in the <user>@<domain> format	—	—
`clone`	Name of an existing server group from which parameter values are copied.	—	—
`no`	Negates any configured parameter.	—	—
`set role|vlan`	Assigns the client a user role or VLAN based on attributes returned for the client by the authentication server. Rules are ordered: the first rule that matches the configured condition is applied.	—	—
`condition`	Attribute returned by the authentication server.	—	—
`contains`	The rule is applied if and only if the attribute value contains the specified string.	—	—
`ends-with`	The rule is applied if and only if the attribute value ends with the specified string.	—	—
`equals`	The rule is applied if and only if the attribute value equals the specified string.	—	—
`not-equals`	The rule is applied if and only if the attribute value is not equal to the specified string.	—	—
`starts-with`	The rule is applied if and only if the attribute value begins with the specified string.	—	—
`set-value`	User role or VLAN applied to the client when the rule is matched.	—	—
`value-of`	Sets the user role or VLAN to the value of the attribute returned. The user role or VLAN ID returned as the value of the attribute must already be configured on the WLAN switch when the rule is applied.	—	—
`position`	Position of the rule relative to other rules for the server group. 1 is the top.	—	(last)

Usage Guidelines

You create a server group for a specific type of authentication or for accounting. The list of servers in a server group is an ordered list, which means that the first server in the group is always used unless it is unavailable (in which case, the next server in the list is used). You can configure servers of different types in a server group, for example, you can include the internal database as a backup to a RADIUS server. You can add the same server to multiple server groups. There is a predefined server group “internal” that contains the internal database.

Example

The following command configures a server group “corp-servers” with a RADIUS server as the main authentication server and the internal database as the backup. The command also sets the client’s user role to the value of the returned “Class” attribute.

```
aaa server-group corp-servers
   auth-server radius1 position 1
   auth-server internal position 2
   set role condition Class value-of
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

aaa sygate-on-demand

```
aaa sygate-on-demand remediation-failure-role <role>
```

Description

This command configures the user role assigned to clients that fail Sygate On-Demand Agent (SODA) remediation.

Syntax

Parameter	Description	Range	Default
`remediation-failure-role`	User role assigned to the client upon failure of client remediation.	—	guest

Usage Guidelines

When you enable SODA client remediation in a captive portal profile, you can specify a user role to clients that fail the remediation. The default role for such clients is the guest role.

Example

The following command assigns the logon role to users who fail remediation:

```
aaa sygate-on-demand remediation-failure-role logon
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Client Integrity license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa tacacs-accounting

```
aaa tacacs-accounting server-group <group> [command {action|all|configuration|show}]
[mode {enable|disable}]
```

Description

This command configures reporting of commands issued on the WLAN switch to a TACACS+ server group.

Syntax

Parameter	Description	Range	Default
`server-group`	The TACACS server group to which the reporting is sent.	—	—
`command`	The types of commands that are reported to the TACACS server group.	—	—
`action`	Reports action commands only.	—	—
`all`	Reports all commands.	—	—
`configuration`	Reports configuration commands only	—	—
`show`	Reports show commands only	—	—
`mode`	Enables accounting for the server group.	enable/ disable	disabled

Usage Guidelines

You must have previously configured the TACACS+ server and server group (see “aaa authentication-server tacacs” on page 33 and “aaa server-group” on page 50).

Example

The following command enables accounting and reporting of configuration commands to the server-group “tacacs1”:

```
aaa tacacs-accounting server-group tacacs1 mode enable command configuration
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa test-server

```
aaa test-server {mschapv2|pap} <server> <username> <passwd>
```

Description

This command tests a configured authentication server.

Syntax

Parameter	Description	Range	Default
`mschapv2`	Use MSCHAPv2 authentication protocol.	—	—
`pap`	Use PAP authentication protocol.	—	—
`<server>`	Name of the configured authentication server.	—	—
`<username>`	Username to use to test the authentication server.	—	—
`<passwd>`	Password to use to test the authentication server.	—	—

Usage Guidelines

This command allows you to check a configured RADIUS authentication server or the internal database. You can use this command to check for an “out of service” RADIUS server.

Example

The following commands adds a user in the internal database and verifies the configuration:

```
local-userdb add kgreen lkjHGfds
aaa test-server pap internal kgreen lkjHGfds

Authentication successful
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa timers

```
aaa timers {dead-time <minutes>|idle-timeout <minutes>|logon-lifetime <minutes>}
```

Description

This command configures the timers you can apply to clients and servers.

Syntax

Parameter	Description	Range	Default
`dead-time`	Maximum period, in minutes, that the WLAN switch considers an unresponsive authentication server to be "out of service". This timer is only applicable if there are two or more authentication servers configured on the WLAN switch. If there is only one authentication server configured, the server is never considered out of service and all requests are sent to the server. If one or more backup servers are configured and a server is unresponsive, it is marked as out of service for the dead time; subsequent requests are sent to the next server on the priority list for the duration of the dead time. If the server is responsive after the dead time has elapsed, it can take over servicing requests from a lower-priority server; if the server continues to be unresponsive, it is marked as down for the dead time.	0-50	10 minutes
`idle-timeout`	Maximum period, in minutes, after which a client is considered idle if there are no new sessions started with the client. The timeout period is reset if there is a new client session. After this timeout period has elapsed, the WLAN switch sends probe packets to the client; if the client responds to the probe, it is considered active and the User Idle Timeout is reset (an active client that is not initiating new sessions is not removed). If the client does not respond to the probe, it is removed from the system. To prevent clients from timing out, set the value in the field to 0.	0-255	5 minutes
`logon-lifetime`	Maximum time, in minutes, that unauthenticated clients are allowed to remain logged on.	0-255	5 minutes

Usage Guidelines

These parameters can be left at their default values for most implementations.

Example

The following command prevents clients from timing out:

```
aaa timers idle-timeout 0
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa trusted-ap

```
aaa trusted-ap <macaddr>
```

Description

This command configures a trusted non-OmniAccess AP.

Syntax

Parameter	Description	Range	Default
`trusted-ap`	MAC address of the AP	—	—

Usage Guidelines

This command configures a non-OmniAccess AP as a trusted AP.

Example

The following configures a trusted non-OmniAccess AP:

```
aaa trusted-ap 00:40:96:4d:07:6e
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa user add

```
aaa user add <ipaddr> [<number>] [authentication-method {dot1x|mac|stateful-dot1x|vpn|
 web}] [mac <macaddr>] [name <username>] [profile <aaa_profile>] [role <role>]
```

Description

This command manually assigns a user role or other values to a specified client or device.

Syntax

Parameter	Description	Range	Default
`<ipaddr>`	IP address of the user to be added.	—	—
`<number>`	Number of users to create starting with <ipaddr>.	—	—
`authentication-method`	Authentication method for the user.	—	—
`dot1x`	802.1x authentication.		
`mac`	MAC authentication.		
`stateful-dot1x`	Stateful 802.1x authentication.		
`vpn`	VPN authentication.		
`web`	Captive portal authentication.		
`mac`	MAC address of the user.	—	—
`name`	Name for the user.	—	—
`profile`	AAA profile for the user.	—	—
`role`	Role for the user.	—	—

Usage Guidelines

This command should only be used for troubleshooting issues with a specific client or device. This command allows you to manually assign a client or device to a role. For example, you can create a role “debugging” that includes a policy to mirror session packets to a specified destination for further examination, then use this command to assign the “debugging” role to a specific client. Use the **aaa user delete** command to remove the client or device from the role.

Note that issuing this command does not affect ongoing sessions that the client may already have. For example, if a client is in the “employee” role when you assign them to the “debugging” role, the client continues any sessions allowed with the “employee” role. Use the **aaa user clear-sessions** command to clear ongoing sessions.

Example

The following commands create a role that logs HTTPS traffic, then assign the role to a specific client:

```
ip access-list session log-https
   any any svc-https permit log
user-role web-debug
   session-acl log-https
```

In enable mode:

```
aaa user add 10.1.1.236 role web-debug
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa user clear-sessions

```
aaa user clear-sessions <ipaddr>
```

Description

This command clears ongoing sessions for the specified client.

Syntax

Parameter	Description	Range	Default
`clear-sessions`	IP address of the user.	—	—

Usage Guidelines

This command clears any ongoing sessions that the client already had before being assigned a role with the **aaa user add** command.

Example

The following command clears ongoing sessions for a client:

```
aaa user clear-sessions 10.1.1.236
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa user delete

```
aaa user delete {<ipaddr>|all|mac <macaddr>|name <username>|role <role>}
```

Description

This command deletes clients, users, or roles.

Syntax

Parameter	Description	Range	Default
`<ipaddr>`	IP address of the client to be deleted.	—	—
`all`	Deletes all connected clients.	—	—
`mac`	MAC address of the client to be deleted.	—	—
`name`	Name of the client to be deleted.	—	—
`role`	Role of the client to be deleted.	—	—

Usage Guidelines

This command allows you to manually delete clients, users, or roles. For example, if you used to the **aaa user add** command to assign a user role to a client, you can use this command to remove the role assignment.

Example

The following command a role:

```
aaa user delete role web-debug
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa user fast-age

```
aaa user fast-age
```

Description

This command enables fast aging of user table entries.

Syntax

No parameters.

Usage Guidelines

When this feature is enabled, the WLAN switch actively sends probe packets to all users with the same MAC address but different IP addresses. The users that fail to respond are purged from the system. This command enables quick detection of multiple instances of the same MAC address in the user table and removal of an “old” IP address. This can occur when a client (or an AP connected to an untrusted port on the WLAN switch) changes its IP address.

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa user logout

```
aaa user logout <ipaddr>
```

Description

This command logs out a client.

Syntax

Parameter	Description	Range	Default
<ipaddr>	IP address of the client to be logged out.	—	—

Usage Guidelines

This command logs out an authenticated client. The client must reauthenticate.

Example

The following command logs out a client:

```
aaa user logout 10.1.1.236
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

aaa xml-api

```
aaa xml-api server <ipaddr>
  clone <server>
  key <key>
  no ...
```

Description

This command configures an external XML API server.

Syntax

Parameter	Description	Range	Default
`server`	IP address of the external XML API server.	—	—
`clone`	Name of an existing XML API server configuration from which parameter values are copied.	—	—
`key`	Preshared key to authenticate communication between the WLAN switch and the XML API server.	—	—
`no`	Negates any configured parameter.	—	—

Usage Guidelines

XML API is used for authentication and subscriber management from external agents. This command configures an external XML API server. For example, an XML API server can send a blacklist request for a client to the WLAN switch. The server configured with this command is referenced in the AAA profile for the WLAN (see "aaa profile" on page 45). Contact your Alcatel-Lucent representative for more information about using the XML API.

Example

The following configures an XML API server:

```
aaa xml-api server 10.210.1.245
  key qwerTYuiOP
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

The External Services Interface license must be installed.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

adp

```
adp discovery {disable|enable} igmp-join {disable|enable} igmp-vlan <vlan>
```

Description

This command configures the Alcatel-Lucent Discovery Protocol (ADP).

Syntax

Parameter	Description	Range	Default
`discovery`	Enables or disables ADP on the WLAN switch.	enabled/ disabled	enabled
`igmp-join`	Enables or disables sending of Internet Group Management Protocol (IGMP) join requests from the WLAN switches.	enabled/ disabled	enabled
`igmp-vlan`	VLAN to which IGMP reports are sent.	—	0 (default route VLAN used)

Usage Guidelines

OmniAccess APs send out periodic multicast and broadcast queries to locate the master WLAN switch. If the APs are in the same broadcast domain as the master WLAN switch and ADP is enabled on the WLAN switch, the WLAN switch automatically responds to the APs' queries with its IP address. If the APs are not in the same broadcast domain as the master WLAN switch, you need to enable multicast on the network. You also need to make sure that all routers are configured to listen for IGMP join requests from the WLAN switch and can route the multicast packets. Use the **show adp config** command to verify that ADP and IGMP join options are enabled on the WLAN switch.

Example

The following example enables ADP and the sending of IGMP join requests on the WLAN switch:

```
adp discovery enable igmp-join enable
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

am

```
am scan <ipaddr> <channel> [bssid <bssid>]
am test <ipaddr> {suspect-rap bssid <bssid> match-type <match-type> match-method
<method>|wired-mac {add|remove {bssid <bssid>|enet-mac <enet-mac>} mac <mac>}
```

Description

These commands enable channel scanning or testing for the specified air monitor.

Syntax

Parameter	Description	Range	Default
`scan`	IP address of the air monitor to be scanned.	—	—
`<channel>`	Channel to which the scanning is tuned. Set to 0 to enable scanning of all channels.	—	—
`bssid`	BSSID of the air monitor.	—	—
`test`	IP address of the air monitor to be tested.	—	—
`suspect-rap`	Tests suspect-rap feature.	—	—
`match-type`	Match type.	eth-wm | ap-wm | eth-gw-wm	—
`match-method`	Match method.	equal | plus-one | minus-one	—
`wired-mac`	Tests the rogue AP classification feature. Specifies the Wired MAC table.	—	—
`enet-mac`	Specifies the Ethernet MAC table.	—	—
`mac`	Specifies the MAC entry to add/remove from either the Wired MAC table or the Ethernet MAC table.	—	—

Usage Guidelines

These commands are intended to be used with an OmniAccess AP that is configured as an air monitor. You should not use the **am test** command unless instructed to do so by an Alcatel-Lucent representative.

Example

The following command sets the air monitor to scan all channels:

```
am scan 10.1.1.244 0
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

Support for the wired-mac and associated parameters was introduced in AOS-W 3.3.1.

ap enet-link-profile

```
ap enet-link-profile <profile>
  clone <profile>
  duplex {auto|full|half}
  no ...
  speed {10|100|1000|auto}
```

Description

This command configures an AP Ethernet link profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`clone`	Name of an existing Ethernet Link profile from which parameter values are copied.	—	—
`duplex`	The duplex mode of the Ethernet interface, either full, half, or auto-negotiated.	full/half/auto	auto
`no`	Negates any configured parameter.	—	—
`speed`	The speed of the Ethernet interface, either 10 Mbps, 100 Mbps, 1000 Mbps (1 Gbps), or auto-negotiated.	10/100/1000/ auto	auto

Usage Guidelines

This command configures the duplex and speed of the Ethernet port on the AP. The configurable speed is dependent on the port type.

Example

The following command configures the Ethernet link profile for full-duplex and 100 Mbps:

```
ap enet-link-profile enet
  duplex full
  speed 100
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

Support for 1000 Mbps (1 Gbps) Ethernet port speed was introduced in AOS-W 3.3.

ap mesh-cluster-profile

```
ap mesh-cluster-profile <profile>
  clone <profile>
  cluster <name>
  no ...
  opmode [opensystem | wpa2-psk-aes]
  rf-band {a | g}
  wpa-hexkey <wpa-hexkey>
  wpa-passphrase <wpa-passphrase>
```

Description

This command configures a mesh cluster profile used by mesh nodes.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`clone`	Name of an existing mesh cluster profile from which parameter values are copied.	—	—
`cluster`	Configures the cluster name, which is used as the mesh service set identifier (MSSID). The cluster name can be up to 32 characters. Each mesh cluster profile should have a unique MSSID.	—	"alcatel-mesh"
`no`	Negates any configured parameter.	—	—
`opmode`	Configures data encryption. ■ opensystem—No authentication and encryption. ■ wpa2-psk-aes—WPA2 with AES encryption using a pershared key. **NOTE:** Alcatel-Lucent recommends selecting wpa2-psk-aes and entering a passphrase (see wpa-passphrase). Keep the passphrase in a safe place.	opensystem/ wpa2-psk-aes	opensystem
`rf-band`	Configures the RF band in which multiband mesh nodes should operate: ■ a = 5 GHz ■ g = 2.4 GHz Alcatel-Lucent recommends using 802.11a radios for mesh deployments.	a/g	a
`wpa-hexkey`	Configures a WPA pre-shared key.	—	—
`wpa-passphrase`	Sets the WPA password that generates the PSK.	—	—

Usage Guidelines

Mesh cluster profiles are specific to mesh nodes (APs configured for mesh) and provide the framework of the mesh network. You must define and configure the mesh cluster profile before configuring an AP to operate as a mesh node.

You can configure multiple mesh cluster profiles to be used within a mesh cluster. You must configure different priority levels for each mesh cluster profile. See "ap-group" on page 91 or "ap-name" on page 94 for more information about priorities.

Cluster profiles, including the “default” profile, are not applied until you provision your APs for mesh.

Viewing Mesh Cluster Profile Settings

To view a complete list of mesh cluster profiles and their status, use the following command:

```
show ap mesh-cluster-profile
```

To view the settings of a specific mesh cluster profile, use the following command:

```
show ap mesh-cluster-profile <name>
```

Example

The following command configures a mesh cluster profile named “cluster1” for the mesh cluster “headquarters:”

```
ap mesh-cluster-profile cluster1
   cluster headquarters
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Secure Enterprise Mesh license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.2.

ap mesh-radio-profile

```
ap mesh-radio-profile <profile>
  11a-portal-channel <channel>
  11g-portal-channel <channel>
  a-tx rates [6|9|12|18|24|36|48|54]
  beacon-period <period>
  children <children>
  clone <profile>
  g-tx rates [1|2|5|6|9|11|12|18|24|36|48|54]
  heartbeat-threshold <count>
  hop-count <hop-count>
  link-threshold <count>
  max-retries <max-retries>
  mesh-mcast-opt
  metric-algorithm {best-link-rssi|distributed-tree-rssi}
  mpv <vlan-id>
  no ...
  reselection-mode {reselect-anytime|reselect-never|startup-subthreshold|
   subthreshold-only}
  rts-threshold <rts-threshold>
  tx-power <tx-power>
```

Description

This command configures a mesh radio profile used by mesh nodes.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`11a-portal-channel`	Configures the 802.11a channel for the mesh portal. The portal's channel decides the channel in which the entire mesh network operates. Valid radio channels are based on your country code. Changing the country code causes the valid channels to be reset to the defaults for the country. Alcatel-Lucent recommends using the 802.11a channel for wireless backhaul between mesh nodes.	—	—
`11g-portal-channel`	Configures the 802.11b/g channel for the mesh portal. The portal's channel decides the channel in which the entire mesh network operates. Valid radio channels are based on your country code. Changing the country code causes the valid channels to be reset to the defaults for the country. Alcatel-Lucent recommends using the 802.11b/g channel for traditional WLAN access.	—	—
`a-tx rates`	Indicates the transmit rates for the 802.11a radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps
`beacon-period`	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the mesh node's presence, identity, and radio characteristics to other mesh nodes.	60-999,999	100 ms
`children`	Indicates the maximum number of children a mesh node can accept.	1-64	64

clone	Name of an existing mesh radio profile from which parameter values are copied.	—	—
g-tx rates	Indicates the transmit rates for the 802.11b/g radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
heartbeat-threshold	Indicates the maximum number of heartbeat messages that can be lost between neighboring mesh nodes.	1-255	10
hop-count	Indicates the maximum hop count from the mesh portal.	1-32	8
link-threshold	Indicates the minimal RSSI value. If the RSSI value is below this threshold, the link may be considered a sub-threshold link. A sub-threshold link is a link whose average RSSI value falls below the configured threshold. If this occurs, the mesh node may try to find a better link on the same channel and cluster (only neighbors on the same channel are considered). The supported threshold is hardware dependent, with a practical range of 10-90.	hardware dependent	12
max-retries	Maximum number of times a mesh node can re-send a packet.	0-15	4 times
mesh-mcast-opt	Enables or disables scanning of all active stations currently associated to a mesh point to select the lowest transmission rate based on the slowest connected mesh child. When enabled, this setting dynamically adjusts the multicast rate to that of the slowest connected mesh child. Multicast frames are not sent if there are no mesh children. Alcatel-Lucent recommends using the default value.		enabled
metric-algorithm	Specifies the algorithm used by a mesh node to select its parent. Alcatel-Lucent recommends using the default value distributed-tree-rssi.	—	distributed-tree-rssi
best-link-rssi	Selects the parent with the strongest RSSI, regardless of the number of children a potential parent has.	—	—
distributed-tree-rssi	Selects the parent based on link-RSSI and node cost based on the number of children. This option evenly distributes the mesh points over high quality uplinks. Low quality uplinks are selected as a last resort.	—	—
mpv	This parameter is experimental and reserved for future use.	0-4094	0 (disabled)
no	Negates any configured parameter.	—	—
reselection-mode	Specifies the method used to find a better mesh link. Alcatel-Lucent recommends using the default value startup-subthreshold.	(see below)	startup-sub threshold
reselect-anytime	Connected mesh nodes evaluate alternative mesh links every 30 seconds. If a mesh node finds a better uplink, the mesh node connects to the new parent to create an improved path to the mesh portal.	—	—
reselect-never	Connected mesh nodes do not evaluate other mesh links to create an improved path to the mesh portal.	—	—

`startup-sub threshold`	When bringing up the mesh network, mesh nodes have 3 minutes to find a better uplink. After that time, each mesh node evaluates alternative links only if the existing uplink falls below the configured threshold level (the link becomes a sub-threshold link). The reselection process is canceled if the average RSSI rises on the existing uplink rises above the configured link threshold.	—	—
`subthreshold -only`	Connected mesh nodes evaluate alternative links only if the existing uplink becomes a sub-threshold link.	—	—
`rts-threshold`	Defines the packet size sent by mesh nodes. Mesh nodes transmitting frames larger than this threshold must issue request to send (RTS) and wait for other mesh nodes to respond with clear to send (CTS) to begin transmission. This helps prevent mid-air collisions.	256-2,346	2,333 bytes
`tx-power`	Sets the maximum transmit power (dBm) on which the AP operates. Enter the value in .5 dBm increments.	0-30	30 dBm

Usage Guidelines

Mesh radio profiles are specific to mesh nodes (APs configured for mesh) and determine the radio frequency/channel used by mesh nodes to establish mesh links and the path to the mesh portal. You can configure multiple radio profiles; however, you select and deploy only one radio profile per mesh cluster.

Radio profiles, including the “default” profile, are not active until you provision your APs for mesh.

NOTE: Mesh radio settings do not apply to thin AP radios.

If you modify a currently provisioned and running radio profile, your changes take place immediately. You do not reboot the WLAN switch or the AP.

Viewing Mesh Radio Profile Settings

To view a complete list of mesh radio profiles and their status, use the following command:

```
show ap mesh-radio-profile
```

To view the settings of a specific mesh radio profile, use the following command:

```
show ap mesh-radio-profile <name>
```

Example

The following command configures a mesh radio profile named “radio1” and configures 56 for the 802.11a portal channel:

```
ap mesh-radio-profile radio1
  11a-channel 56
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Secure Enterprise Mesh license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.2.

The tx-power default increased from 14 to 30 dBm in AOS-W 3.2.0.x, 3.3.1.x, and later builds.

The heartbeat-threshold default increased from 5 to 10 heartbeat messages in AOS-W 3.3.

The mesh-mcast-opt parameter was introduced in AOS-W 3.3.2.

ap regulatory-domain-profile

```
ap regulatory-domain-profile <profile>
  clone <profile>
  country-code <code>
  no ...
  valid-11a-40mhz-channel-pair <num+|num->
  valid-11a-channel <num>
  valid-11g-40mhz-channel-pair <num+|num->
  valid-11g-channel <num>
```

Description

This command configures an AP regulatory domain profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`clone`	Name of an existing regulatory domain profile from which parameter values are copied.	—	—
`country-code`	Code that represents the country in which the APs will operate. The country code determines the 802.11 wireless transmission spectrum. **CAUTION:** Improper country code assignment can disrupt wireless transmissions. Most countries impose penalties and sanctions for operators of wireless networks with devices set to improper country codes.	—	country code configured on the master WLAN switch during initial setup
`no`	Negates any configured parameter.	—	—
`valid-11a-40mhz-channel-pair`	Specifies a channel pair valid for 40 MHz operation in the regulatory domain (determined by country code) for the 5 GHz (802.11a) frequency band. ■ num+: Entering a channel number with a plus (+) sign selects a primary and secondary channel for 40 MHz mode. The number entered becomes the primary channel and the secondary channel is determined by increasing the primary channel number by 4. Example: 157+ represents 157 as the primary channel and 161 as the secondary channel. ■ num-: Entering a channel number with a minus (-) sign selects a primary and secondary channel for 40 MHz mode. The number entered becomes the primary channel and the secondary channel is determined by decreasing the primary channel number by 4. Example: 157- represents 157 as the primary channel and 153 as the secondary channel.	country code determines supported channel pairs **Note:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.	
`valid-11a-channel`	Valid 802.11a channels for the country code. ■ num: Enter a single channel number for 20 MHz mode of operation.	country code determines supported channels **Note:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.	

`valid-11g-40mhz-channel-pair`	Specifies a channel pair valid for 40 MHz operation in the regulatory domain (determined by country code) for the 2.4 GHz (802.11b/g) frequency band. ■ num+: Entering a channel number with a plus (+) sign selects a primary and secondary channel for 40 MHz mode. The number entered becomes the primary channel and the secondary channel is determined by increasing the primary channel number by 4. Example: 1+ represents 1 as the primary channel and 5 as the secondary channel. ■ num-: Entering a channel number with a minus (-) sign selects a primary and secondary channel for 40 MHz mode. The number entered becomes the primary channel and the secondary channel is determined by decreasing the primary channel number by 4. Example: 5- represents 5 as the primary channel and 1 as the secondary channel.	country code determines supported channel pairs **Note:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.
`valid-11g-channel`	Valid 802.11b/g channels for the country code. ■ num: Enter a single channel number for 20 MHz mode of operation.	country code determines supported channels **Note:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.

Usage Guidelines

This profile configures the country code and valid channels for operation of APs. The list of valid channels only affects the channels that may be selected by ARM or by the WLAN switch when no channel is configured. Channels that are specifically configured in the AP radio settings profile (see "rf dot11a-radio-profile" on page 323 or "rf dot11g-radio-profile" on page 326) must be valid for the country.

NOTE: WLAN switches shipped to certain countries, such as the U.S. and Israel, cannot terminate APs with regulatory domain profiles that specify different country codes from the WLAN switch. For example, if a WLAN switch is designated for the U.S., then only a regulatory domain profile with the "US" country code is valid; setting APs to a regulatory domain profile with a different country code will result in the radios not coming up. For WLAN switches in other countries, you can mix regulatory domain profiles on the same WLAN switch; for example, one WLAN switch can support APs in Japan, Taiwan, China, and Singapore.

In order for an AP to boot correctly, the country code configured in the AP regulatory domain profile must match the country code of the LMS.

To view the supported channels, use the **show ap allowed-channels** command.

NOTE: AP configuration settings related to the IEEE 802.11n draft standard are configurable for Alcatel-Lucent OAW-AP120 series access points, which are IEEE 802.11n draft standard compliant devices.

Examples

The following command configures the regulatory domain profile for APs in Japan:

```
ap regulatory-domain-profile rd1
  country-code JP
```

The following command configures a regulatory domain profile for APs in the United States and specifies that the channel pair of 36 and 40, with 36 being the primary channel, is allowed for 40 MHz mode of operation on the 5 GHz frequency band:

```
ap regulatory-domain-profile usa1
  country-code US
  valid-11a-40mhz-channel-pair 36+
```

The following command configures a regulatory domain profile for APs in the United States and specifies that the channel pair of 5 and 1, with 5 being the primary channel, is allowed for 40 MHz mode of operation on the 2.4 GHz frequency band:

```
ap regulatory-domain-profile usa1
  country-code US
  valid-11g-40mhz-channel-pair 5-
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

Support for the IEEE 802.11n draft standard, including channel pairs for 40 MHz mode of operation, was introduced in AOS-W 3.3.

ap snmp-profile

```
ap snmp-profile <profile>
  clone <profile>
  community <community>
  no ...
  snmp-enable
  snmp-user <username>
```

Description

This command configures an SNMP profile for APs.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`clone`	Name of an existing AP SNMP profile from which parameter values are copied.	—	—
`community`	One or more community strings used to authenticate requests for data from the AP. **NOTE:** This is required for SNMP v2c but is not needed for SNMP version 3.	—	—
`no`	Negates any configured parameter.	—	—
`snmp-enable`	Enables or disables SNMP reporting by the OmniAccess AP.	—	enabled
`snmp-user`	One or more existing SNMP user profiles.	—	—

Usage Guidelines

An SNMP profile configures SNMP-related information for OmniAccess APs and can reference one or more instances of SNMP user profiles. OmniAccess WLAN switches and APs support SNMP versions 1, 2c, and 3.

Example

The following command configures an SNMP profile:

```
ap snmp-profile enet
  community trifle
  snmp-enable
  snmp-user admin-mgr
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

ap snmp-user-profile

```
ap snmp-user-profile <profile>
   auth-passwd <password>
   auth-prot {md5|none|sha}
   clone <profile>
   no ...
   priv-passwd <password>
   user-name <name>
```

Description

This command configures an SNMPv3 user profile for APs.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`auth-passwd`	Authentication key for use with the authentication protocol.	—	—
`auth-prot`	The type of authentication protocol used: ■ md5: HMAC-MD5-96 Digest Authentication Protocol ■ none: no authentication is used ■ sha: HMAC-SHA-96 Digest Authentication Protocol	md5/none/ sha	none
`clone`	Name of an existing SNMP user profile from which parameter values are copied.	—	—
`no`	Negates any configured parameter.	—	—
`priv-passwd`	Privacy key for use with the cipher block chaining - data encryption standard (CBC-DES) Symmetric Encryption Protocol.	—	—
`user-name`	String that represents the name of the user.	—	—

Usage Guidelines

The SNMP user profile configures SNMPv3 users.

Example

The following command configures an SNMPv3 user profile:

```
ap snmp-user-profile user1
   user-name ovmmadmin
   auth-prot md5
   auth-passwd 1234567890
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

ap system-profile

```
ap system-profile <profile>
  aeroscout-rtls-server ip-addr <ipaddr> port <port>
  bkup-lms-ip <ipaddr>
  bootstrap-threshold <number>
  clone <profile>
  dns-domain <domain>
  double-encrypt
  dump-server <server>
  heartbeat-dscp <number>
  keepalive-interval <seconds>
  lms-hold-down-period <seconds>
  lms-ip <ipaddr>
  lms-preemption
  maintenance-mode
  master-ip <ipaddr>
  max-request-retries <number>
  mtu <bytes>
  native-vlan-id <vlan>
  no ...
  rap-dhcp-default-router <ipaddr>
  rap-dhcp-dns-server <ipaddr>
  rap-dhcp-lease <days>
  rap-dhcp-pool-end <ipaddr>
  rap-dhcp-pool-netmask <netmask>
  rap-dhcp-pool-start <ipaddr>
  rap-dhcp-server-id <ipaddr>
  rap-dhcp-server-vlan <vlan>
  request-retry-interval <seconds>
  rf-band <band>
  rfprotect-bkup-server <ipaddr>
  rfprotect-server-ip <ipaddr>
  rtls-server ip-addr <ipaddr> port <port> key <key> station-message-frequency
   <seconds>
  session-acl <acl>
  syscontact <name>
  telnet
```

Description

This command configures an AP system profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`aeroscout-rtls-server`	Enables the AP to send RFID tag information to an AeroScout real-time asset location (RTLS) server.	—	—
`ip-addr`	IP address of the AeroScout server to which location reports are sent.	—	—
`port`	Port number on the AeroScout server to which location reports are sent.	—	—
`bkup-lms-ip`	In multi-WLAN switch networks, specifies the IP address of a *backup* to the IP address specified with the lms-ip parameter.	—	—

bootstrap-threshold	Number of consecutive missed heartbeats on a GRE tunnel (heartbeats are sent once per second on each tunnel) before an AP rebootstraps. On the WLAN switch, the GRE tunnel timeout is 1.5 x bootstrap-threshold; the tunnel is torn down after this number of seconds of inactivity on the tunnel.	1-65535	8
clone	Name of an existing AP system profile from which parameter values are copied.	—	—
dns-domain	Name of domain that is resolved by corporate DNS servers. Use this parameter when configuring split tunnel.	—	—
double-encrypt	This parameter applies only to remote APs. Use double encryption for traffic to and from a wireless client that is connected to a tunneled SSID. When enabled, all traffic is re-encrypted in the IPSec tunnel. When disabled, the wireless frame is only encapsulated inside the IPSec tunnel. All other types of data traffic between the WLAN switch and the AP (wired traffic and traffic from a split-tunneled SSID) are always encrypted in the IPSec tunnel.	—	disabled
dump-server	(For debugging purposes.) Specifies the server to receive a core dump generated when an AP process crashes.	—	—
heartbeat-dscp	DSCP value of AP heartbeats.	0-63	0
keepalive-interval	Time, in seconds, between keepalive messages from the AP.	30-65535	60 seconds
lms-hold-down-period	Time, in seconds, that the primary LMS must be available before an AP returns to that LMS after failover.	1-3600	600 seconds
lms-ip	In multi-WLAN switch networks, specifies the IP address of the local management switch (LMS)—the OmniAccess WLAN switch—which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network. This can be the IP address of the local or master WLAN switch. When using redundant WLAN switches as the LMS, set this parameter to be the VRRP IP address to ensure that APs always have an active IP address with which to terminate sessions.	—	—
lms-preemption	Automatically reverts to the primary LMS IP address when it becomes available.	—	disabled
maintenance-mode	Enable or disable AP maintenance mode. **NOTE:** This setting is useful when deploying, maintaining, or upgrading the network. If enabled, APs stop flooding unnecessary traps and syslog messages to network management systems or network operations centers when deploying, maintaining, or upgrading the network. The WLAN switch still generates debug syslog messages if debug logging is enabled.		disabled
master-ip	In multi-WLAN switch networks, specifies the IP address of the master WLAN switch. This address must be reachable by the APs.	—	—
max-request-retries	Maximum number of times to retry AP-generated requests, including keepalive messages. After the maximum number of retries, the AP either tries the IP address specified by the bkup-lms-ip (if configured) or reboots.	1-65535	10
mtu	MTU, in bytes, on the wired link for the AP.	1024-1578	—

native-vlan-id	Native VLAN for bridge mode virtual APs (frames on the native VLAN are not tagged with 802.1q tags).	—	1
no	Negates any configured parameter.	—	—
rap-dhcp-default-router	IP address for the default DHCP router. **NOTE:** The Remote AP license must be installed.		192.168.11.1
rap-dhcp-dns-server	IP address of the DNS server. **NOTE:** The Remote AP license must be installed.		192.168.11.1
rap-dhcp-lease	The amount of days that the assigned IP address is valid for the client. Specify the lease in <days>. 0 indicates the IP address is always valid; the lease does not expire. **NOTE:** The Remote AP license must be installed.	0-30	0
rap-dhcp-pool-end	Configures a DHCP pool for remote APs. This is the last IP address of the DHCP pool. **NOTE:** The Remote AP license must be installed.		192.168.11.254
rap-dhcp-pool-netmask	Configures a DHCP pool for remote APs. This is the netmask used for the DHCP pool. **NOTE:** The Remote AP license must be installed.		255.255.255.0
rap-dhcp-pool-start	Configures a DHCP pool for remote APs. This is the first IP address of the DHCP pool. **NOTE:** The Remote AP license must be installed.		192.168.11.2
rap-dhcp-server-id	IP address used as the DHCP server identifier. **NOTE:** The Remote AP license must be installed.		192.168.11.1
rap-dhcp-server-vlan	VLAN ID of the remote AP DHCP server used if the WLAN switch is unavailable. This VLAN enables the DHCP server on the AP (also known as the remote AP DHCP server VLAN). If you enter the native VLAN ID, the DHCP server is unavailable. **NOTE:** The Remote AP license must be installed.	—	—
request-retry-interval	Interval, in seconds, between the first and second retries of AP-generated requests. If the configured interval is less than 30 seconds, the interval for subsequent retries is increased up to 30 seconds.	1-65535	10 seconds
rf-band	This parameter only applies to AP 60/61. RF band in which the AP should operate: ■ g = 2.4 GHz ■ a = 5 GHz	a/g	g
rfprotect-bkup-server	IP address of the backup RFprotect server. The AP or AP group to which this profile applies operates as an RFprotect sensor.	—	—
rfprotect-server-ip	IP address of the RFprotect server. The AP or AP group to which this profile applies operates as an RFprotect sensor.	—	—
rtls-server	Enables the AP to send RFID tag information to an RTLS server.	—	—
ip-addr	IP address of the server to which location reports are sent.	—	—
port	Port number on the server to which location reports are sent.	—	—
key	Shared secret key.	—	—

station-message-frequency	Indicates how often packets are sent to the server.	5-3600	30 seconds
session-acl	Session ACL configured with the ip access-list session command. **NOTE:** The Policy Enforcement Firewall license must be installed.	—	—
syscontact	SNMP system contact information.	—	—
telnet	Enable or disable telnet to the AP.	—	disabled

Usage Guidelines

The AP system profile configures AP administrative operations, such as logging levels.

Example

The following command sets the LMS IP address in an AP system profile:

```
ap system-profile local1
   lms-ip 10.1.1.240
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for the noted parameters.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

Support for additional RTLS servers, remote AP enhancements was introduced in AOS-W 3.2.

The maintenance-mode parameter was introduced in AOS-W 3.3.

Multiple remote AP DHCP server enhancements were introduced in AOS-W 3.3.2.

Support for RFprotect server and backup server configuration was introduced in AOS-W 3.3.2.

The mms-rtls-server parameter was deprecated in AOS-W 3.3.2. To configure the OV-MM server as an RTLS server, see “mobility-manager” on page 282.

ap wired-ap-profile

```
ap wired-ap-profile <profile>
  clone <profile>
  forward-mode {bridge|split-tunnel|tunnel}
  no ...
  switchport access vlan <vlan>|mode {access|trunk}
   trunk {allowed vlan <list>|add <list>|except <list>|remove <list>
   native vlan <vlan>}
  trusted
  wired-ap-enable
```

Description

This command configures a wired AP profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`clone`	Name of an existing wired AP profile from which parameter values are copied.	—	—
`forward-mode`	Controls whether 802.11 frames are tunneled to the WLAN switch using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the WLAN switch, and Internet access remains local). Only 802.1x authentication is supported when configuring bridge or split tunnel mode. **NOTE:** For split-tunnel mode, the Remote AP license must be installed. **NOTE:** Mesh nodes only support tunnel mode.	bridge/split-tunnel/tunnel	tunnel
`no`	Negates any configured parameter.	—	—
`switchport`	Configures the switching mode characteristics for the port.		
`access`	The VLAN to which the port belongs.	—	1
`mode`	The mode for the port, either access or trunk mode.	access/trunk	access
`trunk allowed`	Allows multiple VLANs on the port interface.	—	all VLANs
`trunk native`	The native VLAN for the port (frames on the native VLAN are not tagged with 802.1q tags).	—	1
`trusted`	Sets port as either trusted or untrusted.	—	untrusted
`wired-ap-enable`	Enables the wired AP.	—	disabled

Usage Guidelines

This command is only applicable to OmniAccess APs that support a second Ethernet port, such as the OAW-AP70. The wired AP profile configures the second Ethernet port (enet1) on the AP.

For mesh deployments, this command is applicable to all OmniAccess APs configured as mesh nodes. If you are using mesh to join multiple Ethernet LANs, configure and enable bridging on the mesh point Ethernet port.

NOTE: Mesh nodes only support bridge mode and tunnel mode on their wired ports (enet0 or enet1). Split tunnel mode is not supported.

Use bridge mode to configure bridging on the mesh point Ethernet port. Use tunnel mode to configure secure jack operation on the mesh node Ethernet port.

When configuring the Ethernet ports on the OAW-AP70, note the following requirements:

- If configured as a mesh portal:
  - Connect enet0 to the WLAN switch to obtain an IP address. The wired AP profile controls enet1.
  - Only enet1 supports secure jack operation.
- If configured as a mesh point, the same wired AP profile will control both enet0 and enet1.

Example

The following command configures the enet1 port on the OAW-AP70 as a trunk port:

```
ap wired-ap-profile wiredap1
   switchport mode trunk
   switchport trunk allowed 4,5
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for the noted parameters.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

Support for split tunneling was introduced in AOS-W 3.2.

ap-group

```
ap-group <group>
  ap-system-profile <profile>
  clone <profile>
  dot11a-radio-profile <profile>
  dot11a-traffic-mgmt-profile <profile>
  dot11g-radio-profile <profile>
  dot11g-traffic-mgmt-profile <profile>
  enet0-profile <profile>
  enet1-profile <profile>
  event-thresholds-profile <profile>
  ids-profile <profile>
  mesh-cluster-profile <profile> priority <priority>
  mesh-radio-profile <profile>
  no ...
  regulatory-domain-profile <profile>
  rf-optimization-profile <profile>
  snmp-profile <profile>
  virtual-ap <profile>
  voip-cac-profile <profile>
  wired-ap-profile <profile>
```

Description

This command configures an AP group.

Syntax

Parameter	Description	Range	Default
`<group>`	Name that identifies the AP group. The name must be 1-63 characters. NOTE: You cannot use quotes (“) in the AP group name.	—	“default”
`ap-system-profile`	Configures AP administrative operations, such as logging levels. See “ap system-profile” on page 84.	—	“default”
`clone`	Name of an existing AP group from which profile names are copied.	—	—
`dot11a-radio-profile`	Configures 802.11a radio settings for the AP group; contains the ARM profile. See “rf dot11a-radio-profile” on page 323.	—	“default”
`dot11a-traffic-mgmt-profile`	Configures bandwidth allocation. See “wlan traffic-management-profile” on page 386.	—	—
`dot11g-radio-profile`	Configures 802.11g radio settings for the AP group; contains the ARM profile. See “rf dot11a-radio-profile” on page 323.	—	“default”
`dot11g-traffic-mgmt-profile`	Configures bandwidth allocation. See “wlan traffic-management-profile” on page 386.	—	—
`enet0-profile`	Configures the duplex and speed of the Ethernet 0 interface on the AP. See “ap enet-link-profile” on page 69.	—	“default”
`enet1-profile`	Configures the duplex and speed of the Ethernet 1 interface on the AP. See “ap enet-link-profile” on page 69.	—	“default”
`event-thresholds-profile`	Configures Received Signal Strength Indication (RSSI) metrics. See “rf event-thresholds-profile” on page 330.	—	“default”
`ids-profile`	Configures Alcatel-Lucent’s Intrusion Detection System (IDS). See “ids profile” on page 181.	—	“default”

`mesh-cluster-profile`	Configures the mesh cluster profile for mesh nodes that are members of the AP group. There is a "default" mesh cluster profile; however, it is not applied until you provision the mesh node. See "ap mesh-cluster-profile" on page 71. **NOTE:** The Secure Enterprise Mesh license must be installed.	—	"default"
`priority`	Configures the priority of the mesh cluster profile. If more than two mesh cluster profiles are configured, mesh points use this number to identify primary and backup profile(s). The lower the number, the higher the priority.	1-16	1
`mesh-radio-profile`	Configures the 802.11g and 802.11a radio settings for mesh nodes that are members of the AP group. See "ap mesh-radio-profile" on page 73. **NOTE:** The Secure Enterprise Mesh license must be installed.	—	"default"
`no`	Negates any configured parameter.	—	—
`regulatory-domain-profile`	Configures the country code and valid channels. See "ap regulatory-domain-profile" on page 77.	—	"default"
`rf-optimization-profile`	Configures load balancing and coverage hole and interference detection. See "rf optimization-profile" on page 335.	—	"default"
`snmp-profile`	Configures SNMP-related parameters. See "ap snmp-profile" on page 80.	—	"default"
`virtual-ap`	One or more profiles, each of which configures a specified WLAN. See "wlan virtual-ap" on page 388.	—	"default"
`voip-cac-profile`	Configures voice over IP (VoIP) call admission control (CAC) options. See "wlan voip-cac-profile" on page 391. **NOTE:** The Voice Services Module license must be installed.	—	"default"
`wired-ap-profile`	Configures the second Ethernet port (enet1) on the AP. See "ap wired-ap-profile" on page 89.	—	"default"

Usage Guidelines

AP groups are at the top of the configuration hierarchy. An AP group collects virtual AP definitions and configuration profiles, which are applied to APs in the group.

Example

The following command configures a virtual AP profile to the "default" AP group:

```
ap-group default
  virtual-ap corpnet
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for the noted parameters.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

Support for the mesh parameters was introduced in AOS-W 3.2.

ap-name

```
ap-name <name>
  ap-system-profile <profile>
  clone <profile>
  dot11a-radio-profile <profile>
  dot11a-traffic-mgmt-profile <profile>
  dot11g-radio-profile <profile>
  dot11g-traffic-mgmt-profile <profile>
  enet0-profile <profile>
  enet1-profile <profile>
  event-thresholds-profile <profile>
  exclude-mesh-cluster-profile-ap <profile>
  exclude-virtual-ap <profile>
  ids-profile <profile>
  mesh-cluster-profile <profile> priority <priority>
  mesh-radio-profile <profile>
  no ...
  regulatory-domain-profile <profile>
  rf-optimization-profile <profile>
  snmp-profile <profile>
  virtual-ap <profile>
  voip-cac-profile <profile>
  wired-ap-profile <profile>
```

Description

This command configures a specific AP.

Syntax

Parameter	Description	Range	Default
<name>	Name that identifies the AP. By default, an AP's name can either be the AP's Ethernet MAC address, or if the AP has been previously provisioned with an earlier version of AOS-W, a name in the format <building>.<floor>.<location>. The name must be 1-63 characters. NOTE: You cannot use quotes (") in the AP name.	—	—
ap-system-profile	Configures AP administrative operations, such as logging levels. See "ap system-profile" on page 84.	—	"default"
clone	Name of an existing AP name from which profile names are copied.	—	—
dot11a-radio-profile	Configures 802.11a radio settings for the AP group; contains the ARM profile. See "rf dot11a-radio-profile" on page 323.	—	"default"
dot11a-traffic-mgmt-profile	Configures bandwidth allocation. See "wlan traffic-management-profile" on page 386.	—	—
dot11g-radio-profile	Configures 802.11g radio settings for the AP group; contains the ARM profile. See "rf dot11a-radio-profile" on page 323.	—	"default"
dot11g-traffic-mgmt-profile	Configures bandwidth allocation. See "wlan traffic-management-profile" on page 386.	—	—
enet0-profile	Configures the duplex and speed of the Ethernet 0 interface on the AP. See "ap enet-link-profile" on page 69.	—	"default"

enet1-profile	Configures the duplex and speed of the Ethernet 1 interface on the AP. See "ap enet-link-profile" on page 69.	—	"default"
event-thresholds-profile	Configures Received Signal Strength Indication (RSSI) metrics. See "rf event-thresholds-profile" on page 330.	—	"default"
exclude-mesh-cluster-profile-ap	Excludes the specified mesh cluster profile from this AP. **NOTE:** The Secure Enterprise Mesh license must be installed.	—	—
exclude-virtual-ap	Excludes the specified virtual AP profiles from this AP.		
ids-profile	Configures Alcatel-Lucent's Intrusion Detection System (IDS). See "ids profile" on page 181.	—	"default"
mesh-cluster-profile	Configures the mesh cluster profile for the AP (mesh node). There is a "default" mesh cluster profile; however, it is not applied until you provision the mesh node. See "ap mesh-cluster-profile" on page 71. **NOTE:** The Secure Enterprise Mesh license must be installed.	—	"default"
priority	Configures the priority of the mesh cluster profile. If more than two mesh cluster profiles are configured, mesh points use this number to identify primary and backup profile(s). The lower the number, the higher the priority.	1-16	1
mesh-radio-profile	Configures the 802.11g and 802.11a radio settings for the AP (mesh node). See "ap mesh-radio-profile" on page 73. **NOTE:** The Secure Enterprise Mesh license must be installed.	—	"default"
no	Negates any configured parameter.	—	—
regulatory-domain-profile	Configures the country code and valid channels. See "ap regulatory-domain-profile" on page 77.	—	"default"
rf-optimization-profile	Configures load balancing and coverage hole and interference detection. See "rf optimization-profile" on page 335.	—	"default"
snmp-profile	Configures SNMP-related parameters. See "ap snmp-profile" on page 80.	—	"default"
virtual-ap	One or more profiles, each of which configures a specified WLAN. See "wlan virtual-ap" on page 388.	—	"default"
voip-cac-profile	Configures voice over IP (VoIP) call admission control (CAC) options. See "wlan voip-cac-profile" on page 391. **NOTE:** The Voice Services Module license must be installed.	—	"default"
wired-ap-profile	Configures the ports for APs that are directly attached to the WLAN switch. See "ap wired-ap-profile" on page 89.	—	"default"

Usage Guidelines

Profiles that are applied to an AP group can be overridden on a per-AP name basis, and virtual APs can be added or excluded on a per-AP name basis. If a particular profile is overridden for an AP, all parameters from the overriding profile are used. There is no merging of individual parameters between the AP and the AP group to which the AP belongs.

Example

The following command excludes a virtual AP profile from a specific AP:

```
ap-name 00:0b:86:c0:cf:d8
   exclude-virtual-ap corpnet
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for the noted parameters.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

Support for the mesh parameters was introduced in AOS-W 3.2.

ap-regroup

```
ap-regroup {ap-name <name>|serial-num <num>|wired-mac <macaddr>} <group>
```

Description

This command moves a specified AP into a group.

Syntax

Parameter	Description	Range	Default
`ap-name`	Name of the AP.	—	—
`serial-num`	Serial number of the AP.	—	—
`wired-mac`	MAC address of the AP.	—	—
`<group>`	Name that identifies the AP group. The name must be 1-63 characters.	—	“default”

Usage Guidelines

All APs discovered by the WLAN switch are assigned to the “default” AP group. An AP can belong to only one AP group at a time. You can move an AP to an AP group that you created with the **ap-group** command.

NOTE: This command automatically reboots the AP.

Example

The following command moves an AP to the ‘corpnet’ group:

```
ap-regroup wired-mac 00:0f:1e:11:00:00 corpnet
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

ap-rename

```
ap-rename {ap-name <name>|serial-num <num>|wired-mac <macaddr>} <new-name>
```

Description

This command changes the name of an AP to the specified new name.

Syntax

Parameter	Description	Range	Default
`ap-name`	Current name of the AP.	—	—
`serial-num`	Serial number of the AP.	—	—
`wired-mac`	MAC address of the AP.	—	—
`<new-name>`	New name for the AP. The name must be 1-63 characters. NOTE: You cannot use quotes (“) in the AP name.	—	—

Usage Guidelines

An AP name must be unique within your network.

NOTE: This command automatically reboots the AP.

Example

The following command renames an AP:

```
ap-rename wired-mac 00:0f:1e:11:00:00 building3-lobby
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

apboot

```
apboot {all [global|local]|ap-group <group> [global|local]|ap-name <name>|ip-addr
<ipaddr>|wired-mac <macaddr>}
```

Description

This command reboots the specified APs.

Syntax

Parameter	Description	Range	Default
`all`	Reboot all APs.	—	—
`global`	Reboot APs on all WLAN switches.	—	—
`local`	Reboot only APs registered on this WLAN switch. This is the default.	—	—
`ap-group`	Reboot APs in a specified group.	—	—
`global`	Reboot APs on all WLAN switches.	—	—
`local`	Reboot only APs registered on this WLAN switch. This is the default.	—	—
`ap-name`	Reboot the AP with the specified name.	—	—
`ip-addr`	Reboot the AP at the specified IP address.	—	—
`wired-mac`	Reboot the AP at the specified MAC address.	—	—

Usage Guidelines

You should not normally need to use this command as APs automatically reboot when you reprovision them. Use this command only when directed to do so by your Alcatel-Lucent representative.

Example

The following command reboots a specific AP:

```
apboot ap-name Building3-Lobby
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

apdisconnect

```
apdisconnect {ap-name <name>|bssid <bssid>|ip-addr <ipaddr>}
```

Description

This command disconnects a mesh point from its parent.

Syntax

Parameter	Description	Range	Default
`ap-name`	Specifies the name of the parent AP.	—	—
`bssid`	Specifies the BSSID of the parent AP.	—	—
`ip-addr`	Specifies the IP address of the parent AP.	—	—

Usage Guidelines

Each mesh point learns about the mesh portal from its parent (a mesh node that is part of the path to the mesh portal). This command directs a mesh point to disassociate from its parent. The mesh point will attempt to associate with another neighboring mesh node, if available. The old parent is not eligible for re-association for 60 seconds after disconnection.

Example

The following command disconnects a specific mesh point from its parent:

```
apdisconnect ap-name meshpoint1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Secure Enterprise Mesh license.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.2.

apflash

```
apflash {ap-name <name>|ip-addr <ipaddr>|wired-mac <macaddr>} [backup-partition]
[server <ipaddr>]
```

Description

This command reflashes the specified AP.

Syntax

Parameter	Description	Range	Default
`ap-name`	Reflash the AP with the specified name.	—	—
`ip-addr`	Reflash the AP at the specified IP address.	—	—
`wired-mac`	Reflash the AP at the specified MAC address.	—	—
`backup-partition`	(OAW-AP80 only) Reflash partion 2.	—	—
`server`	IP address of the FTP server.	—	—

Usage Guidelines

This command directs an AP to download its image from the WLAN switch. You should not normally need to run this command, as OmniAccess APs automatically download their images from a WLAN switch during bootup.

Example

The following command reflashes a specific AP:

```
apflash ap-name Building3-Lobby
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

arp

```
arp <ipaddr> <macaddr>
```

Description

This command adds a static Address Resolution Protocol (ARP) entry.

Syntax

Parameter	Description	Range	Default
`<ipaddr>`	IP address of the device to be added.	—	—
`<macaddr>`	Hardware address of the device to be added, in the format xx:xx:xx:xx:xx:xx.	—	—

Usage Guidelines

If the IP address does not belong to a valid IP subnetwork, the ARP entry is not added. If the IP interface that defines the subnetwork for the static ARP entry is deleted, you will be unable to use the arp command to overwrite the entry's current values; use the no arp command to negate the entry and then enter a new arp command.

Example

The following command configures an ARP entry:

```
arp 10.152.23.237 00:0B:86:01:7A:C0
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

audit-trail

```
audit-trail [all]
```

Description

This command enables an audit trail.

Syntax

Parameter	Description	Range	Default
`all`	Enables audit trail for all commands, including enable mode commands. The **audit-trail** command without this option enables audit trail for all commands in configuration mode.	—	—

Usage Guidelines

By default, audit trail is enabled for all commands in configuration mode.

Use the **show audit-trail** command to display the content of the audit trail.

Example

The following command enables an audit trail:

```
audit-trail
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

backup

```
backup {flash|pcmcia}
```

Description

This command backs up compressed critical files in flash.

Syntax

Parameter	Description	Range	Default
`flash`	Backs up flash directories to flashbackup.tar.gz file.	—	—
`pcmcia`	Backs up flash images to external PCMCIA flash card. This option can only be executed on WLAN switches that have a PCMCIA slot.	—	—

Usage Guidelines

Use the **restore flash** command to untar and uncompress the flashbackup.tar.gz file.

Example

The following command backs up flash directories to the flashbackup.tar.gz file:

```
backup flash
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

banner motd

```
banner motd <delimiter> <textString>
```

Description

This command defines a text banner to be displayed at the login prompt when a user accesses the WLAN switch.

Syntax

Parameter	Description	Range	Default
`<delimiter>`	Indicates the beginning and end of the banner text.	—	—
`<textString>`	The text you want displayed.	up to 1023 characters	—

Usage Guidelines

The banner you define is displayed at the login prompt to the WLAN switch. The banner is specific to the WLAN switch on which you configure it. The WebUI displays the configured banner at its login prompt, but you cannot use the WebUI to configure the banner.

The delimiter is a single character that indicates the beginning and the end of the text string in the banner. Select a delimiter that is not used in the text string you define, because the WLAN switch ends the banner when it sees the delimiter character repeated.

There are two ways of configuring the banner message:

- Enter a space between the delimiter and the beginning of the text string. The text can include any character except a quotation mark (“). Use quotation marks to enclose your text if you are including spaces (spaces are not recognized unless your text string is enclosed in quotation marks; without quotation marks, the text is truncated at the first space). You can also use the delimiter character within quotation marks.
- Press the **Enter** key after the delimiter to be placed into a mode where you can simply enter the banner text in lines of up to 255 characters, including spaces. Quotation marks are ignored.

Examples

The following example configures a banner by enclosing the text within quotation marks:

```
banner motd * “Welcome to my WLAN switch. This WLAN switch is in the production
network, so please do not save configuration changes. Maintenance will be performed at
7:30 PM, so please log off before 7:00 PM.”*
```

The following example configures a banner by pressing the **Enter** key after the delimiter:

```
banner motd *
Enter TEXT message [maximum of 1023 characters].
Each line in the banner message should not exceed 255 characters.
End with the character '*'.

Welcome to my WLAN switch. This WLAN switch is in the production network, so please do
not save configuration changes. Maintenance will be performed at 7:30 PM, so please log
off before 7:00 PM.*
```

The banner display is as follows:

```
Welcome to my WLAN switch. This WLAN switch is in the production network, so please do
not save configuration changes. Maintenance will be performed at 7:30 PM, so please log
off before 7:00 PM.
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 1.0.

boot

```
boot
  cf-test [fast | read-only | read-write]
  config-file <filename>
  system partition [0 | 1]
  verbose
```

Description

This command configures the boot options for the WLAN switch.

Syntax

Parameter	Description	Range	Default
`cf-test`	Sets the type of compact flash test to run when booting the WLAN switch.	—	—
`fast`	Performs a fast test, which does not include media testing.	—	—
`read-only`	Performs a read-only media test.	—	—
`read-write`	Performs a read-write media test.	—	—
`config-file`	Sets the configuration file to use when booting the WLAN switch.	—	—
`<filename>`	Specifies the name of the configuration file from which to boot the WLAN switch.	—	—
`system`	Specifies the system partition to use when booting the WLAN switch.	—	—
`0 | 1`	Indicates the partition to use as either 0 or 1. One of the partitions is the active partition and the other is the backup.	—	—
`verbose`	Prints extra debugging information at boot.	—	—

Usage Guidelines

Use the following options to control the boot behavior of the WLAN switch:

- `cf-test`—Test the flash during boot.
- `config-file`—Set the configuration file to use during boot.
- `system`—Specify the system partition to use during boot.
- `verbose`—Print extra debugging information during boot. The information is sent to the screen at boot time. Printing the extra debugging information is disabled using the `no boot verbose` command.

Example

The following command uses the configuration file january-config.cfg the next time the WLAN switch boots:

```
boot config-file january-config.cfg
```

The following command uses system partition 1 the next time the WLAN switch boots:

```
boot system partition 1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode.

History

This command was available in AOS-W 1.0.

cfgm

```
cfgm {mms config {enable|disable}|set config-chunk <kbytes>|set heartbeat
<seconds>|set maximum-updates <number>|snapshot-timer <minutes>}
```

Description

This command configures the configuration module on the master WLAN switch.

Syntax

Parameter	Description	Range	Default
`mms config`	Permits OmniVista Mobility Manager (OV-MM) configuration updates on the master WLAN switch. When enabled, global configuration changes can only be done from OV-MM and are not available on the master WLAN switch.	enablel disable	disabled
`config-chunk`	Maximum packet size, in Kbytes, that is sent every second to the local WLAN switch whenever the master WLAN switch sends a configuration to the local. If the connection between the master and local is slow or uneven, you can lower the size to reduce the amount of data that needs to be retransmitted. If the connection is very fast and stable, you can increase the size to make the transmission more efficient.	1-100	10 Kbytes
`heartbeat`	Interval, in seconds, at which heartbeats are sent. You can increase the interval to reduce traffic load.	10-300	10 seconds
`maximum-updates`	Maximum number of local WLAN switches that can be updated at the same time with configuration changes. You can decrease this value if you have a busy network. You can increase this value to improve configuration synchronization.	2-25	5
`snapshot-timer`	Interval, in minutes, that the local WLAN switch waits for a configuration download from the master upon bootup or startup before loading the last snapshot configuration.	5-60	5 minutes

Usage Guidelines

By default, OV-MM configuration updates on the WLAN switch are disabled to prevent any alterations to the WLAN switch configuration. You need to explicitly enable OV-MM configuration updates for the WLAN switch to accept configuration changes from OV-MM. When OV-MM configuration updates are enabled, global configuration changes can only be done from OV-MM and are not available on the master WLAN switch. You can use the **cfgm mms config disable** command if the WLAN switch loses connectivity to the OmniVista Mobility Manager server and you must enter a configuration change on the master WLAN switch.

Example

The following command allows configuration updates from the OmniVista Mobility Manager:

```
cfgm mms config enable
```

Platform Availability

This command is available on all platforms. This command is available only on master WLAN switches.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.1.

clock set

`clock set <year><month><day><time>`

Description

This command sets the date and time.

Syntax

Parameter	Description	Range	Default
`year`	Sets the year. Requires all 4 digits.	Numeric	—
`month`	Sets the month. Requires the 1st 3 letters of the month.	Alphabetic	—
`day`	Sets the day.	1-31	—
`time`	Sets the time. Specify hours, minutes, and seconds separated by spaces.	Numeric	—

Usage Guidelines

You can configure the year, month, day, and time. You must configure all four parameters.

Specify the time using a 24-hour clock. You must specify the seconds.

Example

The following example configures the clock to January 1st of 2007, at 1:03:52 AM.

```
clock set 2007 jan 1 1 3 52
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was introduced in AOS-W 1.0.

clock summer-time

```
clock summer-time <WORD> [recurring]
  <1-4> <start day> <start month> <hh:mm>
  first <start day> <start month> <hh:mm>
  last <start day> <start month> <hh:mm>
  <1-4> <end day> <end month> <hh:mm>
  first <end day> <end month> <hh:mm>
  last <end day> <end month> <hh:mm>
  [<-23 - 23>]
```

Description

This command sets daylight savings time.

Syntax

Parameter	Description	Range	Default
WORD	Name of the time zone.	3-5 characters	—
1-4	Week of the month when the time change takes effect.	1-4	—
first	Time change takes effect on the first week of the month.	—	—
last	Time change takes effect on the last week of the month.	—	—
start day	Day of the week when the time change takes effect.	Sunday-Saturday	—
start month	Month when the time change takes effect.	January-December	—
hh:mm	Time when the time change takes effect.	24 hours	—
-23 - 23	Hours offset from UTC.	-23 - 23	—

Usage Guidelines

This command subtracts exactly 1 hour from the configured time.

The WORD can be any alphanumeric string, but cannot start with a colon (:). A WORD longer than five characters is not accepted. If you enter a WORD containing punctuation, the command is accepted, but the timezone is set to UTC.

You can configure the time to change on a recurring basis. To do so, set the week, day, month, and time when the change takes effect (daylight savings time starts). You must also set the week, day, month, and time when the time changes back (daylight savings time ends).

The start day requires the first three letters of the day. The start month requires the first three letters of the month.

You also have the option to set the number of hours by which to offset the clock from UTC. This has the same effect as the “clock timezone” command.

Example

The following example sets daylight savings time to occur starting at 2:00 AM on Sunday in the second week of March, and ending at 2:00 AM on Sunday in the first week of November. The example also sets the name of the time zone to PST with an offset of UTC - 8 hours.

```
clock summer-time PST recurring 2 Sun Mar 2:00 first Sun Nov 3:00 -8
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 1.0.

clock timezone

```
clock timezone <WORD> <-23 - 23>
```

Description

This command sets the timezone on the WLAN switch.

Syntax

Parameter	Description	Range	Default
WORD	Name of the time zone.	3-5 characters	—
-23 - 23	Hours offset from UTC.	-23 - 23	—

Usage Guidelines

The WORD can be any alphanumeric string, but cannot start with a colon (:). A WORD longer than five characters is not accepted. If you enter a WORD containing punctuation, the command is accepted, but the timezone is set to UTC.

Example

The following example configures the timezone to PST with an offset of UTC - 8 hours.

```
clock timezone PST -8
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 1.0.

configure terminal

```
configure terminal
```

Description

This command allows you to enter configuration commands.

Syntax

No parameters.

Usage Guidelines

Upon entering this command, the enable mode prompt changes to:

```
(host) (config) #
```

To return to enable mode, enter Ctrl-Z or **exit**.

Example

The following command allows you to enter configuration commands:

```
configure terminal
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode.

History

This command was available in AOS-W 3.0.

copy

```
copy
flash: <srcfilename> {flash: <destfilename> | scp: <scphost> <username> <destfilename> |
   tftp: <tftphost> <destfilename>} |
ftp: <ftphost> <user> <filename> system: partition {0|1} |
running-config {flash: <filename> | ftp: <ftphost> <user> <password> <filename>
   [<remote-dir>] | startup-config | tftp: <tftphost> <filename>} |
scp: <scphost> <username> <filename> {flash: <destfilename>| system: partition [0|1]}|
startup-config {flash: <filename> | tftp: <tftphost> <filename>} |
system: partition {<srcpartition> 0|1} [<destpartition> 0 | 1] |
tftp: <tftphost> <filename> {flash: <destfilename> | system: partition [0|1]}
```

Description

This command copies files to-and-from the WLAN switch.

Syntax

Parameter	Description
`flash:`	Copy the contents of the WLAN switch's flash file system, the system image, to a specified destination.
`srcfilename`	Full name of the flash file to be copied.
`flash:`	Copy the file to the flash file system.
`destfilename`	Specify the new name of the copied file.
`tftp:`	Copy the file to a TFTP server.
`tftphost`	Specify the IP address or hostname of the TFTP server.
`ftp:`	Copy a file from the FTP server.
`ftphost`	Specify the IP address or hostname of the FTP server.
`user`	User account name required to access the FTP server.
`filename`	Full name of the file to be copied.
`0 | 1`	Specify the system partition to save the file.
`running-config`	Copy the active, running configuration to a specified destination.
`flash:`	Copy the configuration to the flash file system.
`filename`	Specify the new name of the copied configuration file.
`ftp:`	Using FTP, copy the configuration to an FTP server.
`ftphost`	Specify the IP address of the FTP server.
`user`	User account name required to access the FTP server.
`password`	Password required to access the FTP server.
`remote-dir`	Specify a remote directory, if needed.
`startup-config`	Copy the active, running configuration to the start-up configuration.
`tftp:`	Using TFTP, copy the configuration to a TFTP server
`tftphost`	Specify the IP address or hostname of the TFTP server.
`scp:`	Copy an AOS-W image file or file from the flash file system using the Secure Copy protocol. The SCP server or remote host must support SSH version 2 protocol.
`scphost`	Specify the IP address of the SCP server or remote host.

Parameter	Description
username	User account name required to access the SCP server or remote host.
filename	Specify the absolute path of the filename to be copied.
flash:	Copy the file to the flash file system.
destfilename	Specify the new name of the copied file.
system:	Copy the file to the system partition.
startup-config	Copy the startup configuration to a specified flash file or to a TFTP server.
flash:	Copy the file to the flash file system.
filename	Specify the new name of the copied startup configuration file.
tftp:	Using TFTP, copy the startup configuration to a TFTP server
tftphost	Specify the IP address or hostname of the TFTP server.
system:	Copy the specified system partition
srcpartition	Disk partition from which to copy the system data, as either 0 or 1.
destpartition	Disk partition to copy the system data to, as either 0 or 1.
tftp:	Copy a file from the specified TFTP server to either the WLAN switch or another destination. This command is typically used when performing a system restoration, or to pull a specified file name into the wms database.
tftphost	Specify the IP address or hostname of the TFTP server.
filename	Full name of the file to be copied.
flash:	Copy the file to the flash file system
destfilename	Specify the new name of the copied file.
system	Copy the file to the system partition.

Usage Guidelines

Use this command to save back-up copies of the configuration file to an FTP or TFTP server, or to load a saved file from an FTP or TFTP server.

Three partitions reside on the file system flash. Totalling 256MB, the three partitions provide space to hold the system image files (in partitions 1 and 2 which are 45MB each) and user files (in partition 3, which is 165MB). System software runs on the system partitions; the database, DHCP, startup configuration, and logs are positioned on the user partition.

To restore a database, copy the database from the network server and import the database.

To restore a configuration file, copy the file from network server to the WLAN switch's flash system then copy the file from the flash system to the system configuration. This ensures that you do not accidentally overwrite your system startup configuration file.

Example

The following commands copy the configuration file named engineering from the TFTP server to the WLAN switch's flash file system and then uses that file as the startup configuration. This example assumes the startup configuration file is named default.cfg:

```
copy tftp: 192.0.2.0 engineering flash: default.bak
copy flash: default.bak flash: default.cfg
```

The following commands restore the system database. You must copy the database to the WLAN switch and run the import database command:

```
copy tftp: 192.0.2.0 flash: wms.db
wms import-db wms.db
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable and config modes on master WLAN switches.

History

This command was available in AOS-W 1.0.

copy log

```
copy log <type> <ipaddress> <userid>
```

Description

This command copies the specified log file to the destination address.

Syntax

Parameter	Description	Range	Default
`type`	Specify the log to transfer. The following logs are available, among others: ■ all—Copies all log files ■ ap-debug—Copies AP debug logs ■ bssid-debug—Copies BSSID logs ■ error-log—Copies errors logged in the system ■ essid-debug—Copies ESSID logs ■ network—Copies network logs ■ security—Copies security logs ■ system—Copies system logs ■ user—Copies user logs ■ user-debug—Copies user debug logs ■ wireless—Copies wireless logs **NOTE:** You may see slightly different logs depending on the WLAN switch and the software you are using.	—	—
`ipaddress`	Specify the IP address of the destination.	—	—
`userid`	User account name required to access the destination.	—	—

Usage Guidelines

The transferred file is named `type`.*log*.

Example

The following command copies the wireless logs to a network FTP server:

```
copy log wireless x.x.x.x administrator
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable and config modes on master WLAN switches.

History

This command was available in AOS-W 1.0.

crypto dynamic-map

```
crypto dynamic-map <name> <priority>
  no ...
  set pfs {group1|group2}
  set security-association lifetime seconds <seconds>
  set transform-set <name1> [<name2>] [<name3>] [<name4>]
```

Description

This command configures a dynamic map.

Syntax

Parameter	Description	Range	Default
<name>	Name of the map.	—	—
<priority>	Priority of the map.	1-10000	10000
no	Negates a configured parameter.	—	—
pfs	Enables Perfect Forward Secrecy (PFS) mode. Use one of the following:	group1/ group2	disabled
	group1: 768-bit Diffie Hellman prime modulus group		
	group2: 1024-bit Diffie Hellman prime modulus group		
seconds	Configures the lifetime, in seconds, for the security association (SA).	300-86400	no limit
transform-set	Name of the transform set for this dynamic map. You can specify up to four transform sets. You configure transform sets with the crypto ipsec transform-set command.	—	default-trans form

Usage Guidelines

Dynamic maps enable IPSec SA negotiations from dynamically addressed IPSec peers.

Example

The following command configures a dynamic map:

```
crypto dynamic-map dmap1 100
  set pfs group2
  set security-association lifetime seconds 300
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server and/or Remote AP license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

crypto ipsec

```
crypto ipsec mtu <mtu> | transform-set <name> {esp-3des|esp-aes128|esp-aes192|
esp-aes256|esp-des} (esp-md5-hmac|esp-sha-hmac}
```

Description

This command configures IPSec MTU size and transform sets.

Syntax

Parameter	Description	Range	Default
`mtu`	Configures the maximum transmission unit.	1024-1500	1500
`transform-set`	Name of the transform set. Specify the encryption and authentication algorithm.	—	default-transform
`esp-3des`	Use ESP with 168-bit 3DES encryption. This is the default with the default-transform set.	—	—
`esp-aes128`	Use ESP with 128-bit AES encryption.	—	—
`esp-aes192`	Use ESP with 192-bit AES encryption.	—	—
`esp-aes256`	Use ESP with 256-bit AES encryption.	—	—
`esp-des`	Use ESP with 56-bit DES encryption.	—	—
`esp-md5-hmac`	Use ESP with MD5 authentication algorithm.	—	—
`esp-sha-hmac`	Use ESP with SHA authentication algorithm. This is the default with the default-transform set.	—	—

Usage Guidelines

A transform set specifies a combination of authentication and encryption methods.

Example

The following command configures a transform set:

```
crypto ipsec transform-set ts1 esp-aes128 esp-sha-hmac
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server and/or Remote AP license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

crypto isakmp

```
crypto isakmp groupname <name> | key <key> address <ipaddr> netmask <mask>
```

Description

This command configures IKE on the WLAN switch.

Syntax

Parameter	Description	Range	Default
`address`	IP address to which the preshared key applies. To configure a single key for all clients, specify 0.0.0.0.	—	—
`netmask`	Netmask for the IP address. To configure a single key for all clients, specify 0.0.0.0.	—	—
`groupname`	IKE aggressive group name.	—	—
`key`	Preshared key, between 6-64 characters, for the peer group. The key must match the value configured on the client.	—	—

Usage Guidelines

This command configures the IKE preshared key to be used for a group of IP addresses (or for all clients). To configure an IKE policy, see “crypto isakmp policy” on page 126.

Example

The following command configures a global preshared key for all clients:

```
crypto isakmp key myK3y$ address 0.0.0.0 netmask 0.0.0.0
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server and/or Remote AP license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

crypto isakmp packet-dump

```
crypto isakmp packet-dump
```

Description

This command enables ISAKMP protocol packet dumps.

NOTE: This command is used for testing purposes only and should not be enabled for production deployments.

Syntax

Parameter	Description	Range	Default
`packet-dump`	Enables packet dumps.	—	—

Usage Guidelines

Enable this command only when directed to do so by an Alcatel-Lucent representative. The ISAKMP messages sent on the control path during VPN negotiation are stored in the /var/log/oslog/ike.pcap file. Please turn off the packet dump as soon as troubleshooting is completed using the command **no crypto isakmp packet-dump**.

NOTE: This command is used for testing purposes only and should not be enabled for production deployments.

Example

The following command enables packet dumps:

```
crypto isakmp packet-dump
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server and/or Remote AP license.

Command Mode

This command is available in enable mode.

History

This command was available in AOS-W 3.0.

crypto isakmp policy

```
crypto isakmp policy <priority>
   authentication {pre-share|rsa-sig}
   encryption {3DES|AES128|AES192|AES256|DES}
   group {1|2}
   hash {md5|sha}
   lifetime <seconds>
```

Description

This command configures an IKE policy.

Syntax

Parameter	Description	Range	Default
policy	Priority of the IKE policy. 1 is the highest priority.	1-10000	—
authentication	IKE authentication method.	pre-share/ rsa-sig	pre-share
pre-share	Use preshared keys.	—	—
rsa-sig	Use RSA signatures. Specify this option for certificate-based IKE.	—	—
encryption	IKE encryption algorithm.	—	3DES
3DES	Use 168-bit 3DES-CBC encryption.	—	—
AES128	Use 128-bit AES-CBC encryption.	—	—
AES192	Use 192-bit AES-CBC encryption.	—	—
AES256	Use 256-bit AES-CBC encryption.	—	—
DES	Use 56-bit DES-CBC encryption.	—	—
group	IKE Diffie Hellman group.	1/2	2
1	Use 768-bit Diffie Hellman prime modulus group.	—	—
2	Use 1024-bit Diffie Hellman prime modulus group.	—	—
hash	IKE hash algorithm.	md5/sha	sha
md5	Use MD5.	—	—
sha	Use SHA-1.	—	—
lifetime	IKE lifetime, in seconds.	300-86400	(no volume limit)

Usage Guidelines

An IKE policy defines a combination of authentication, encryption, and other parameters used during IKE negotiation.

Example

The following command configures an IKE policy:

```
crypto isakmp policy 100
   encryption AES128
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server and/or Remote AP license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

crypto isakmp psk-caching

```
crypto isakmp psk-caching {days <interval_days> | hours <interval_hours>} {disable}
```

Description

This command enables preshared key (PSK)-refresh for remote APs.

Syntax

Parameter	Description	Range	Default
`days`	Number of days to remember the previously configured preshared key.	1-365	—
`hours`	Number of hours to remember the previously configured preshared key.	2-24	—
`disable`	Disables PSK-refresh.	—	—

Usage Guidelines

By default, PSK-refresh is disabled. To enable PSK-refresh, you must:

1. Configure the amount of time in days or hours (known as the interval), to remember the previously configured PSK used in your remote AP deployment.

   NOTE: Alcatel-Lucent recommends configuring a large interval to prevent remote APs from being unable to authenticate and connect to the network. Consider your existing PSK interval when configuring this feature.

2. Configure the global PSK. The IP address must be 0.0.0.0, and the netmask must be 0.0.0.0.

   NOTE: If you do not configure the global PSK, the PSK-refresh feature is invalid.

   For more information about configuring the global PSK, see "crypto isakmp" on page 124.

NOTE: If a remote AP attempts authentication with an expired PSK, the WLAN switch generates an error message similar to the following: `Dropping RAP IKE request from IP:<address> Port:<number> because old PSK is invalid`. If this occurs, you must reprovision the remote AP.

Disabling PSK-Refresh

To disable PSK-refresh, use one of the following commands:

```
crypto isakmp psk-caching disable
no crypto isakmp psk-caching
```

Viewing PSK-Refresh Settings

To display the current PSK-refresh setting, use the following command:

```
show crypto isakmp psk-caching
```

Example

The following command enables IKE PSK-refresh by specifying the number of days the WLAN switch remembers the previously configured PSK:

```
crytpo isakmp psk-caching days 125
```

To configure the global psk:

```
crypto isakmp key myRap$ address 0.0.0.0 netmask 0.0.0.0
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server and the Remote AP license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.3.2.

crypto map

```
crypto map global-map <priority> ipsec-isakmp {dynamic <map>|ipsec <map>}
```

Description

This command configures the default global map.

Syntax

Parameter	Description	Range	Default
`global-map`	Priority of the map.	—	—
`ipsec-isakmp`	Configures the IPSec map.	—	—
`dynamic`	Use the specified dynamic map.	—	—
`ipsec`	Use the specified IPSec map.	—	—

Usage Guidelines

Use the **crypto dynamic-map** command to configure a dynamic map. Use the **crypto-local ipsec-map** command to configure an IP Sec map for site-to-site VPN.

Example

The following command configures the global map:

```
crypto map global-map 100 ipsec-isakmp dynamic dmap1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server and/or Remote AP license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

crypto pki csr

```
crypto pki csr key {1024|2048|4096} common_name <value> country <country>
state_or_province <state> city <city> organization <org> unit <string> email <email>
```

Description

This command generates a Certificate Signing Request (CSR) which you can send to a certificate authority (CA) to obtain a signed certificate.

Syntax

Parameter	Description	Range	Default
key	Length of private/public key.	1024/2048/4096	—
common_name	This must be a fully-qualified domain name, as in yourhost.yourcompany.com.	—	—
country	Two-letter ISO country code for the country in which your organization is located. The country code must be in the format specified by the ISO 3166 standard (http://www.niso.org/standards/resources/3166.html).	—	—
state_or_province	State, province, region, or territory in which your organization is located.	—	—
city	City in which your organization is located.	—	—
organization	Name of your organization.	—	—
unit	Optional field to distinguish a department or other unit within your organization.	—	—
email	Email address referenced in the CSR.	—	—

Usage Guidelines

This command also generates a private key with the CSR. After you generate the CSR, copy and paste the CSR into an email and send it to the CA (use the CLI command 'show crypto pki csr' to display the CSR). When you receive the signed certificate from the CA, import it into the WLAN switch using the WebUI.

NOTE: There can be only one outstanding CSR at a time in the WLAN switch.

Example

The following command generates a CSR:

```
crypto pki key 1024 common-name www.yourcompany.com country us state_or_province CA
city "San Jose" organization "YourCompany Inc." unit Engineering email
root@yourcompany.com
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was introduced in AOS-W 3.1.

crypto pki-import

```
crypto pki-import {der|pem|pfx|pkcs12} {PublicCert|ServerCert|TrustedCA} <certificate>
<filename> [<passphrase>]
```

Description

This command is used by the WebUI for importing certificates.

NOTE: All certificates that are not generated by the WLAN switch must be imported using the WebUI.

Syntax

Parameter	Description	Range	Default
`der`	Imports a DER format certificate.	—	—
`pem`	Imports a X.509 PEM format certificate.	—	—
`pfx`	Imports a PKCS12 (PFX) format certificate.	—	—
`pkcs12`	Imports a PKCS12 format certificate.	—	—
`PublicCert`	Imports a public certificate.	—	—
`ServerCert`	Imports a server certificate.	—	—
`TrustedCA`	Imports a trusted CA certificate.	—	—
`<certificate>`	Name of the certificate.	—	—
`<filename>`	Imported filename of the certificate.	—	—
`<passphrase>`	Optional passphrase used during import to store the certificate's private key.	—	—

Usage Guidelines

This command is not for general use.

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

crypto-local ipsec-map

```
crypto-local ipsec-map <map> <priority>
  dst-net <ipaddr> <mask>
  no ...
  peer-ip <ipaddr>
  pre-connect {disable|enable}
  set ca-certificate <cacert-name>
  set pfs {group1|group2}
  set security-association lifetime seconds <seconds>
  set server-certificate <cert-name>
  set transform-set <name1> [<name2>] [<name3>] [<name4>]
  src-net <ipaddr> <mask>
  trusted {disable|enable}
  vlan <vlan>
```

Description

This command configures IPSec mapping for site-to-site VPN.

Syntax

Parameter	Description	Range	Default
<map>	Name of the IPSec map.	—	—
<priority>	Priority of the entry.	1-9998	—
ca-certificate	User-defined name of a trusted CA certificate installed in the WLAN switch. Use the **show crypto-local pki TrustedCA** command to display the CA certificates that have been imported into the WLAN switch.	—	—
dst-net	IP address and netmask for the destination network.	—	—
no	Negates a configured parameter.	—	—
peer-ip	IP address of the peer gateway.	—	—
pre-connect	Enables or disables pre-connection.	enable/ disable	disabled
pfs	Enables Perfect Forward Secrecy (PFS) mode. Use one of the following: group1: 768-bit Diffie Hellman prime modulus group group2: 1024-bit Diffie Hellman prime modulus group	group1/ group2	disabled
seconds	Configures the lifetime, in seconds, for the security association (SA).	300-86400	no limit
server-certificate	User-defined name of a server certificate installed in the WLAN switch. Use the **show crypto-local pki ServerCert** command to display the server certificates that have been imported into the WLAN switch.	—	—
transform-set	Name of the transform set for this IPSec map. You can specify up to four transform sets. You configure transform sets with the crypto ipsec transform-set command.	—	default-transform
src-net	IP address and netmask for the source network.	—	—
trusted	Enables or disables a trusted tunnel.	enable/ disable	disabled
vlan	VLAN ID. Enter 0 for the loopback.	1-4094	—

Usage Guidelines

You can use WLAN switches instead of VPN concentrators to connect sites at different physical locations. For site-to-site VPN between two WLAN switches, you must purchase and install VPN Server licenses on both WLAN switches.

You can configure separate CA and server certificates for each site-to-site VPN. You can also configure the same CA and server certificates for site-to-site VPN and client VPN. Use the **show crypto-local ipsec-map** command to display the certificates associated with all configured site-to-site VPN maps; use the **tag <map>** option to display certificates associated with a specific site-to-site VPN map.

Example

The following commands configures site-to-site VPN between two WLAN switches:

```
crypto-local ipsec-map sf-chi-vpn 100
   src-net 101.1.1.0 255.255.255.0
   dst-net 100.1.1.0 255.255.255.0
   peer-ip 172.16.0.254
   vlan 1
   trusted

crypto-local ipsec-map chi-sf-vpn 100
   src-net 100.1.1.0 255.255.255.0
   dst-net 101.1.1.0 255.255.255.0
   peer-ip 172.16.100.254
   vlan 1
   trusted
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

crypto-local isakmp ca-certificate

```
crypto-local isakmp ca-certificate <cacert-name>
```

Description

This command assigns the Certificate Authority (CA) certificate used to authenticate VPN clients.

Syntax

Parameter	Description	Range	Default
`ca-certificate`	User-defined name of a trusted CA certificate installed in the WLAN switch. Use the **show crypto-local pki TrustedCA** command to display the CA certificates that have been imported into the WLAN switch.	—	—

Usage Guidelines

You can assign multiple CA certificates. Use the **show crypto-local isakmp ca-certificate** command to view the CA certificates associated with VPN clients.

Example

This command configures a CA certificate:

```
crypto-local isakmp ca-certificate TrustedCA1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server license.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 3.2.

crypto-local isakmp dpd

```
crypto-local isakmp dpd idle-timeout <seconds> retry-timeout <seconds>  retry-attempts
<number>
```

Description

This command configures IKE Dead Peer Detection (DPD) on the local WLAN switch.

Syntax

Parameter	Description	Range	Default
`idle-timeout`	Idle timeout, in seconds.	10-3600	22 seconds
`retry-timeout`	Retry interval, in seconds.	2-60	2 seconds
`retry-attempts`	Number of retry attempts.	3-10	3

Usage Guidelines

DPD is enabled by default on the WLAN switch for site-to-site VPN.

Example

This command configures DPD parameters:

```
crypto-local isakmp dpd idle-timeout 60 retry-timeout 3 retry-attempts 5
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server and/or Remote AP licenses.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

crypto-local isakmp key

```
crypto-local isakmp key <key> address <peer-ipaddr> netmask <mask>
```

Description

This command configures the IKE preshared key on the local WLAN switch for site-to-site VPN.

Syntax

Parameter	Description	Range	Default
`key`	IKE preshared key value, between 6-64 characters.	—	—
`address`	IP address for the preshared key.	—	—
`netmask`	Netmask for the preshared key.	—	—

Usage Guidelines

This command configures the IKE preshared key.

Example

The following command configures an IKE preshared key for site-to-site VPN:

```
crypto-local isakmp key R8nD0mK3y address 172.16.100.1 netmask 255.255.255.255
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server and/or Remote AP licenses.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

crypto-local isakmp permit-invalid-cert

```
crypto-local isakmp permit-invalid-cert
```

Description

This command allows invalid or expired certificates to be used for site-to-site VPN.

Syntax

No parameters.

Usage Guidelines

This command allows invalid or expired certificates to be used for site-to-site VPN.

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server and/or Remote AP licenses.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 3.2.

crypto-local isakmp server-certificate

```
crypto-local isakmp server-certificate <cert-name>
```

Description

This command assigns the server certificate used to authenticate the WLAN switch for VPN clients.

Syntax

Parameter	Description	Range	Default
`server-certificate`	User-defined name of a server certificate installed in the WLAN switch. Use the **show crypto-local pki ServerCert** command to display the server certificates that have been imported into the WLAN switch.	—	—

Usage Guidelines

This certificate is only for VPN clients and not for site-to-site VPN clients. You can assign only one server certificate for use with VPN clients. Use the **show crypto-local isakmp server-certificate** command to view the server certificate associated with VPN clients. You must import and configure server certificates separately on master and local WLAN switches.

NOTE: There is a default server certificate installed in the WLAN switch, however this certificate does not guarantee security for production networks. Alcatel-Lucent strongly recommends that you replace the default certificate with a custom certificate issued for your site or domain by a trusted CA. You can use the WebUI to generate a Certificate Signing Request (CSR) to submit to a CA and then import the signed certificate received from the CA into the WLAN switch. For more information, see “Managing Certificates” in the *AOS-W User Guide*.

Example

This command configures a server certificate:

```
crypto-local isakmp server-certificate ServerCert1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server license.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 3.2.

crypto-local isakmp xauth

```
crypto-local isakmp xauth
```

Description

This command enables IKE XAuth for VPN clients.

Syntax

No parameters.

Usage Guidelines

The **no crypto-local isakmp xauth** command disables IKE XAuth for VPN clients. This command only applies to VPN clients that use certificates for IKE authentication. If you disable XAuth, then a VPN client that uses certificates will not be authenticated using username/password. You must disable XAuth for Cisco VPN clients using CAC Smart Cards.

Example

This command disables IKE XAuth for Cisco VPN clients using CAC Smart Cards:

```
no crypto-local isakmp xauth
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server license.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 3.2.

crypto-local pki

```
crypto-local pki {PublicCert|ServerCert|TrustedCA} <name> <filename>
```

Description

This command is saved in the configuration file when you import a certificate from the WebUI.

NOTE: All certificates that are not generated by the WLAN switch need to be imported from the WebUI.

Syntax

Parameter	Description	Range	Default
`PublicCert`	Public key of a certificate. This allows an application to identify an exact certificate.	—	—
`ServerCert`	Server certificate. This certificate must contain both a public and a private key (the public and private keys must match). You can import a server certificate in either PKCS12 or x509 PEM format; the certificate is stored in x509 PEM DES encrypted format on the WLAN switch.	—	—
`TrustedCA`	Trusted CA certificate. This can be either a root CA or intermediate CA. Alcatel-Lucent encourages (but does not require) an intermediate CA's signing CA to be the WLAN switch itself.	—	—
`<name>`	Name of the certificate.	—	—
`<filename>`	Internal directory structure in the WLAN switch in which the imported certificate is stored.	—	—

Usage Guidelines

This command in the configuration file verifies the presence of the certificate in the WLAN switch's internal directory structure.

Platform Availability

This command appears on all platforms.

Licensing Requirements

This command appears in the base operating system.

Command Mode

This command appears in the configuration file after you import a certificate using the WebUI.

History

This command was introduced in AOS-W 3.1.

database synchronize

```
database synchronize
```

Description

This command manually synchronizes the database between a pair of redundant master WLAN switches.

Syntax

No parameters.

Usage Guidelines

This command takes effect immediately. If a peer is not configured, the WLAN switch displays an error message.

Use the **database synchronize period** command in config mode to configure the interval for automatic database synchronization.

Example

The following command causes the database on the active master WLAN switch to synchronize with the standby:

```
database synchronize
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode.

History

This command was available in AOS-W 3.0.

database synchronize period

```
database synchronize period <minutes>
```

Description

This command configures periodic database synchronization between a pair of redundant master WLAN switches.

Syntax

Parameter	Description	Range	Default
`period`	Interval, in minutes, at which the database is synchronized.	1-25200	disabled

Usage Guidelines

Use the **master-redundancy** command to configure redundant master WLAN switches. Use this command to cause the database on the active master WLAN switch to synchronize with the standby during the predefined interval.

To ensure successful synchronization of database events, you should set the interval to a minimum period of 20 minutes.

Example

The following command configures database synchronization:

```
database synchronize period 60
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

database synchronize rf-plan-data

```
database synchronize rf-plan-data
```

Description

This command specifies that RF plan data is included the database is synchronized between a pair of redundant master WLAN switches.

Syntax

No parameters.

Usage Guidelines

Use the **master-redundancy** command to configure redundant master WLAN switches. Use the **database synchronize** command to cause the database on the active master WLAN switch to synchronize with the standby.

Example

The following command includes RF plan data in the database synchronization:

```
database synchronize rf-plan-data
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

delete

```
delete {filename <filename>|ssh-host-addr <ipaddr>|ssh-known-hosts}
```

Description

This command deletes a file or RSA signature entry from flash.

Syntax

Parameter	Description	Range	Default
`filename`	Name of the file to be deleted.	—	—
`ssh-host-addr`	Deletes the entry stored in flash for the RSA host signature created when you run the **copy scp** command.	—	—
`ssh-known -hosts`	Deletes all entries stored in flash for the RSA host signatures created when you run the **copy scp** command.	—	—

Usage Guidelines

To prevent running out of flash file space, you should delete files that you no longer need.

The **copy scp** command creates RSA signatures whenever it connects to a new host. These host signatures are stored in the flash file system.

Examples

The following command deletes a file:

```
delete filename december-config-backup.cfg
```

The following command deletes an RSA signature entry from flash:

```
delete ssh-host-addr 10.100.102.101
```

The following command deletes all RSA signature entries from flash:

```
delete ssh-known-hosts
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

destination

```
destination <STRING> <A.B.C.D> [invert]
```

Description

This command configures the destination name and address.

Syntax

Parameter	Description	Range	Default
`STRING`	Destination name.	Alphanumeric	—
`A.B.C.D`	Destination IP address or subnet.	—	—
`invert`	Specifies all destinations except this one.	—	—

Usage Guidelines

You can configure the name and IP address of the destination. You can optionally configure the subnet, or invert the selection.

Example

The following example configures a destination called “Home” with an IP address of 10.10.10.10.

```
destination Home 10.10.10.10
```

Platform Availability

This command is only available on the master WLAN switch.

Licensing Requirements

This command requires the Policy Enforcement Firewall license.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 1.0.

This command was replaced in AOS-W 3.0 with the `netdestination` command.

dir

```
dir
```

Description

This command displays a list of files stored in the flash file system.

Syntax

No parameters.

Usage Guidelines

Use this command to view the system files associated with the WLAN switch.

Output from this command includes the following:

- The first column contains ten place holders that display the file permissions
  - First place holder—Displays `-` for a file or `d` for directory
  - Next three place holders—Display file owner permissions: `r` for read access, `w` for write access permissions, `x` for executable
  - Following three place holders—Display member permissions: `r` for read access or `x` for executable
  - Last three place holders—Display non-member permissions: `r` for read access or `x` for executable
- The second column displays the number of links the file has to other files or directories
- The third column displays the file owner
- The fourth column displays group/member information
- The remaining columns display the file size, date and time the file was either created or last modified, and the file name

Example

The following command displays the files currently residing on the system flash:

```
dir
```

The following is sample output from this command:

```
-rw-r--r--    1 root     root         9338 Nov 20 10:33 class_ap.csv
-rw-r--r--    1 root     root         1457 Nov 20 10:33 class_sta.csv
-rw-r--r--    1 root     root        16182 Nov 14 09:39 config-backup.cfg
-rw-r--r--    1 root     root        14174 Nov  9  2005 default-backup-11-8-05.cfg
-rw-r--r--    1 root     root        16283 Nov  9 12:25 default.cfg
-rw-r--r--    1 root     root        22927 Oct 25 12:21 default.cfg.2006-10-25_20-21-38
-rw-r--r--    2 root     root        19869 Nov  9 12:20 default.cfg.2006-11-09_12-20-22
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable and config modes on master WLAN switches.

History

This command was available in AOS-W 1.0.

dynamic-ip

```
dynamic-ip restart
```

Description

This command restarts the PPPoE or DHCP process.

Syntax

No parameters.

Usage Guidelines

This command can be used to renegotiate DHCP or PPPoE parameters. This can cause new addresses to be assigned on a VLAN where the DHCP or PPPoE client is configured.

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode.

History

This command was available in AOS-W 3.0.

enable

```
enable
```

Description

This user mode command switches the WLAN switch into enable mode.

Usage Guidelines

To enter enable mode, you are prompted for the password configured during the WLAN switch's initial setup. Passwords display as asterisks (*) when you enter them. To change the password, use the config mode "enable secret" command. If you lose or forget the enable mode password, resetting the default admin user password also resets the enable mode password to "enable". See the *AOS-W User Guide* for more information about resetting the admin and enable mode passwords.

When you are in enable mode, the CLI prompt ends with the hash (#) character.

Example

The following example allows you to enter enable mode on the WLAN switch.

```
(host) >enable
Password: ******
(host) #
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in user mode.

History

This command was introduced in AOS-W 1.0.

enable secret

```
enable secret
```

Description

This config mode command allows you to change the password for enable mode.

Usage Guidelines

Use this command to change the password for enable mode. To reset the password to the factory default of “enable”, use the `no enable` command.

NOTE: The password must not contain the space and ‘?’ special characters.

Example

The following example allows you to change the password for enable mode.

```
(host) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(host) (config) #enable secret
Password:******
Re-Type password: ******
(host) (config) #
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 1.0.

Restriction of the secret phrase was introduced in AOS-W 3.3.2.

encrypt

```
encrypt {disable|enable}
```

Description

This command allows passwords and keys to be displayed in plain text or encrypted.

Syntax

Parameter	Description	Default
`disable`	Passwords and keys are displayed in plain text.	—
`enable`	Passwords and keys are displayed encrypted.	enabled

Usage Guidelines

Certain commands, such as **show crypto isakmp key**, display configured key information. Use the **encrypt** command to display the key information in plain text or encrypted.

Example

The following command allows passwords and keys to be displayed in plain text:

```
encrypt disable
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode.

History

This command was available in AOS-W 3.0.

esi group

```
esi group <name>
   [no] |
   [ping <attributes>] |
   [server <server>]
```

Description

This command configures an ESI group.

Syntax

Parameter	Description	Range	Default
`no`	Negates any configured parameter.	—	—
`ping`	Specify ping checking attributes. Only one set is allowed.	—	—
`server`	Specify a server to be added to or removed from the server group.	—	—

Usage Guidelines

Use the `show esi group` command to show ESI group information.

Example

The following command sets up the ESI group named “fortinet.”

```
esi group fortinet
   ping default
   server forti_1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the External Services Interface license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 2.5.

esi parser domain

```
esi parser domain <name>
   [no] |
   [peer <peer-ip>] |
   [server <ipaddr>]
```

Description

This command configures an ESI syslog parser domain.

Syntax

Parameter	Description	Range	Default
`no`	Negates any configured parameter.	—	—
`peer`	(Optional.) Specify the IP address of an another WLAN switch in this domain. These WLAN switches are notified when the user cannot be found locally. This command is needed only when multiple WLAN switches share a single ESI server.	—	—
`server`	Specify the IP address of the ESI server to which the WLAN switch listens.	—	—

Usage Guidelines

The ESI parser is a generic syslog parser on the WLAN switch that accepts syslog messages from external third-party appliances such as anti-virus gateways, content filters, and intrusion detection systems. It processes syslog messages according to user-defined rules and takes configurable actions on the corresponding system users.

ESI servers (see "esi server" on page 163) are configured into domains to which ESI syslog parser rules (see "esi parser rule" on page 157) are applied.

Use the `show esi parser domains` command to show ESI parser domain information.

Example

The following commands configure a virus syslog parser domain named "fortinet" which contains the ESI server "forti_1" with the trusted IP address configured using the command "esi server" on page 163.

```
esi parser domain fortinet
   server 10.168.172.3
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the External Services Interface license.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 3.1.

esi parser rule

```
esi parser rule <rule_name>
   [condition <expression>] |
   [domain <name>] |
   [enable]
   [match {ipaddr <expression> | mac <expression> | user <expression> }] |
   [no] |
   [position <position>] |
   [set {blacklist | role <role>} |
   [test {msg <msg> | file <filename>}]
```

Description

This command creates or changes an ESI syslog parser rule.

Syntax

Parameter	Description	Range	Default
`condition`	Specifies the REGEX (regular expression) pattern that uniquely identifies the syslog.	—	—
`domain`	(Optional.) Specify the ESI syslog parser domain to which this rule applies. If not specified, the rule matches with all configured ESI servers.	—	—
`enable`	Enables this rule. **Note**: The condition, user match, and set action parameters must be configured before the rule can be enabled.	—	Not enabled
`match`	Specifies the user identifier to match, where `ipaddr`, `mac`, and `user` take a REGEX pattern that uniquely identifies the user.	—	—
`no`	Negates any configured parameter.	—	—
`position`	Specifies the rule's priority position.	1–32; 1 highest	—
`set`	Specifies the action to take: blacklist the user or change the user role. **Note**: The role entity should be configured before it is accepted by the ESI rule.	—	—
`test`	Test the regular expression output configured in the `esi parser rules` command. You can test the expressions against a specified syslog message, or test the expression against a sequence of syslog messages contained in a file.	—	—

Usage Guidelines

The user creates an ESI rule by using characters and special operators to specify a pattern that uniquely identifies a syslog message. This "condition" defines the type of message and the ESI domain to which this message pertains. The rule contains three major fields:

- Condition: The pattern that uniquely identifies the syslog message type.
- User: The username identifier. It can be in the form of a name, MAC address, or IP address.
- Action: The action to take when a rule match occurs.

Once a condition match occurs, no further rule-matching will be made. For the matching rule, only one action can be defined.

For more details on the character-matching operators, repetition operators, and expression anchors used to defined the search or match target, see the External Services Interface chapter in the *AOS-W User Guide*.

Use the `show esi parser rules` command to show ESI parser rule information. Use the `show esi parser stats` command to show ESI parser rule statistical information

Examples

The following command sets up the Fortigate virus rule named “forti_rule.” This rule parses the virus detection syslog scanning for a condition match on the log_id value (log_id=) and a match on the IP address (src=).

```
esi parser rule forti_rule
   condition “log_id=[0-9]{10}[ ]”
   match ipaddr “src=(.*)[ ]”
   set blacklist
   domain fortinet
   enable
```

In this example, the corresponding ESI expression is:

```
< Sep 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
```

The following example of the test command tests a rule against a specified single syslog message.

```
test msg "26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4"

< 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
=====
Condition:     Matched with rule "forti_rule"
User:          ipaddr = 1.2.3.4
=====
```

The following example of the test command tests a rule against a file named test.log, which contains several syslog messages.

```
test file test.log

 < Sep 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
==========
Condition:      Matched with rule "forti_rule"
User:           ipaddr = 1.2.3.4
==========

 < Oct 18 10:43:40  cli[627]: PAPI_Send: To: 7f000001:8372 Type:0x4 Timed out. >
==========
Condition:      No matching rule condition found
==========

 < Oct 18 10:05:32  mobileip[499]: <500300> <DBUG> |mobileip|  Station 00:40:96:a6:a1:a4,
10.0.100.103: DHCP FSM received event: RECEIVE_BOOTP_REPLY current: PROXY_DHCP_NO_PROXY,
next: PROXY_DHCP_NO_PROXY >
==========
Condition:      No matching rule condition found
==========
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the External Services Interface license.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 3.1.

esi parser rule-test

```
esi parser rule-test
   [file <filename>] |
   [msg <msg>]
```

Description

This command allows you to test all of the enabled parser rules.

Syntax

Parameter	Description	Range	Default
file	Tests against a specified file containing more than one syslog message.	—	—
msg	Tests against a syslog message, where <msg> is the message text.	—	—

Usage Guidelines

You can test the enabled parser rules against a syslog message input, or run the expression through a file system composed of syslog messages. The command shows the match result as well as the user name parsed for each message.

Example

The following command tests against a specified single syslog message.

```
esi parser rule-test msg
"26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4"

< 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
=====
Condition:     Matched with rule "forti_rule"
User:          ipaddr = 1.2.3.4
=====
```

The following command tests against a file named test.log, which contains several syslog messages.

```
esi parser rule-test file test.log

 < Sep 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
==========
Condition:      Matched with rule "forti_rule"
User:           ipaddr = 1.2.3.4
==========

 < Oct 18 10:43:40  cli[627]: PAPI_Send: To: 7f000001:8372 Type:0x4 Timed out. >
==========
Condition:      No matching rule condition found
==========
```

```
 < Oct 18 10:05:32  mobileip[499]: <500300> <DBUG> |mobileip|  Station 00:40:96:a6:a1:a4,
10.0.100.103: DHCP FSM received event: RECEIVE_BOOTP_REPLY current: PROXY_DHCP_NO_PROXY,
next: PROXY_DHCP_NO_PROXY >
==========
Condition:      No matching rule condition found
==========
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the External Services Interface license.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 3.1.

esi ping

```
esi ping <ping-name>
   [frequency <seconds>] |
   [no] |
   [retry-count <count>] |
   [timeout <seconds>] |
```

Description

This command specifies the ESI ping health check configuration.

Syntax

Parameter	Description	Range	Default
`frequency`	Specifies the ping frequency in seconds.	1–65536	5
`no`	Negates any configured parameter.	—	—
`retry-count`	Specifies the ping retry count.	1–65536	2
`timeout`	Specifies the ping timeout in seconds.	1–65536	2

Usage Guidelines

Use the `show esi ping` command to show ESI ping information.

Example

The following command specifies the ping health check attributes.

```
esi ping default
   frequency 5
   retry-count 2
   timeout 2
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the External Services Interface license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 2.5.

esi server

```
esi server <name>
   [dport <tcp-udp-port>] |
   [mode {bridge | nat | route}] |
   [no] |
   [trusted-ip-addr <ip-addr> [health-check]] |
   [trusted-port <slot/port>] |
   [untrusted-ip-port <ip-addr> [health-check]] |
   [untrusted-port <slot/port>]
```

Description

This command configures an ESI server.

Syntax

Parameter	Description	Range	Default
`dport`	Specifies the NAT destination TCP/UDP port.	—	—
`mode`	Specifies the ESI server mode of operation: bridge, nat, or route.	—	—
`no`	Negates any configured parameter.	—	—
`trusted-ip-addr`	Specifies the server IP address on the trusted network. As an option, you can also enable a health check on the specified address.	—	—
`trusted-port`	Specifies the port connected to the trusted side of the ESI server; slot/port format.	—	—
`untrusted-ip-addr`	Specifies the server IP address on the untrusted network. As an option, you can also enable a health check on the specified address.	—	—
`untrusted-port`	Specifies the port connected to the untrusted side of the ESI server.	—	—

Usage Guidelines

Use the `show esi server` command to show ESI server information.

Example

The following command specifies the ESI server attributes.

```
esi server forti_1
   mode route
   trusted-ip-addr 10.168.172.3
   untrusted-ip-addr 10.168.171.3
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the External Services Interface license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 2.5.

exit

```
exit
```

Description

This command exits the current CLI mode.

Syntax

No parameters.

Usage Guidelines

Upon entering this command in a configuration sub-mode, you are returned to the configuration mode. Upon entering this command in configuration mode, you are returned to the enable mode. Upon entering this command in enable mode, you are returned to the user mode. Upon entering this command in user mode, you are returned to the user login.

Example

The following sequence of **exit** commands return the user from the interface configuration sub-mode to the user login:

```
(host) (config-if)#exit
(host) (config) #exit
(host) #exit
(host) >exit
User:
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in user, enable, configuration, and configuration sub-modes.

History

This command was available in AOS-W 3.0.

export

```
export gap-db <filename>
```

Description

This command exports the global AP database to the specified file.

Syntax

Parameter	Description	Range	Default
<filename>	Name of the file to which the global AP database is exported.	—	—

Usage Guidelines

This command is intended for system troubleshooting. You should run this command only when directed to do so by an Alcatel-Lucent support representative.

The global AP database resides on a master WLAN switch and contains information about known APs on all WLAN switches in the system. You can view the contents of the global AP database with the **show ap database** command.

Example

The following command exports the global AP database to a file:

```
export gap-db global-ap-db
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

firewall

```
firewall {allow-tri-session |attack-rate {ping <number>|session <number>|
tcp-syn <number>} |deny-inter-user-bridging |disable-ftp-server |
disable-stateful-sip |drop-ip-fragments |enable-per-packet-logging |
enforce-tcp-handshake |gre-call-id-processing |log-icmp-error |
prohibit-ip-spoofing |prohibit-rst-replay |session-idle-timeout <seconds> |
session-mirror-destination {ip-address <ipaddr>|port <slot>/<port>} |voip-proxy-arp
|wmm-voip-content-enforcement}
```

Description

This command configures firewall options on the WLAN switch.

Syntax

Parameter	Description	Range	Default
`allow-tri-session`	Allows three-way session when performing destination NAT. This option should be enabled when the WLAN switch is not the default gateway for wireless clients and the default gateway is behind the WLAN switch. This option is typically used for captive portal configuration.	—	disabled
`attack-rate`	Sets rates which, if exceeded, can indicate a denial of service attack.		
`ping`	Number of ICMP pings per second, which if exceeded, can indicate a denial of service attack. Recommended value is 4	1-255	—
`session`	Number of TCP or UDP connection requests per second, which if exceeded, can indicate a denial of service attack. Recommended value is 32.	1-255	—
`tcp-syn`	Number of TCP SYN messages per second, which if exceeded, can indicate a denial of service attack. Recommended value is 32.	1-255	—
`deny-inter-user-bridging`	Prevents the forwarding of Layer-2 traffic between wired or wireless users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic. This option can be used to prevent traffic, such as Appletalk or IPX, from being forwarded.	—	disabled
`disable-ftp-server`	Disables the FTP server on the WLAN switch. Enabling this option prevents FTP transfers. **NOTE:** Enabling this option could cause APs to not boot up. You should not enable this option unless instructed to do so by an Alcatel-Lucent representative.	—	disabled
`disable-stateful-h323-processing`	Disables stateful H.323 processing.	—	enabled
`disable-stateful-sip`	Disables monitoring of exchanges between a voice over IP or voice over WLAN device and a SIP server. This option should be enabled only when thee is no VoIP or VoWLAN traffic on the network.	—	disabled
`drop-ip-fragments`	When enabled, all IP fragments are dropped. You should not enable this option unless instructed to do so by an Alcatel-Lucent representative.	—	disabled

enable-per-packet-logging	Enables logging of every packet if logging is enabled for the corresponding session rule. Normally, one event is logged per session. If you enable this option, each packet in the session is logged. You should not enable this option unless instructed to do so by an Alcatel-Lucent representative, as doing so may create unnecessary overhead on the WLAN switch.	—	disabled
enforce-tcp-handshake	Prevents data from passing between two clients until the three-way TCP handshake has been performed. This option should be disabled when you have mobile clients on the network as enabling this option will cause mobility to fail. You can enable this option if there are no mobile clients on the network.	—	disabled
gre-call-id-processing	Creates a unique state for each PPTP tunnel. You should not enable this option unless instructed to do so by an Alcatel-Lucent representative.	—	disabled
local-valid-users	If this option is enabled then the IP addresses that belong to a local subnet will be added to the user-table.	—	disabled
log-icmp-error	Logs received ICMP errors. You should not enable this option unless instructed to do so by an Alcatel-Lucent representative.	—	disabled
prohibit-ip-spoofing	Detects IP spoofing (where an intruder sends messages using the IP address of a trusted client). When this option is enabled, IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.	—	disabled
prohibit-rst-replay	Closes a TCP connection in both directions if a TCP RST is received from either direction. You should not enable this option unless instructed to do so by an Alcatel-Lucent representative.	—	disabled
session-idle-timeout	Time, in seconds, that a non-TCP session can be idle before it is removed from the session table. You should not modify this option unless instructed to do so by an Alcatel-Lucent representative.	16-259	15 seconds
session-mirror-destination	Destination to which mirrored packets are sent. This option is used only for troubleshooting or debugging. Packets can be mirrored in multiple ACLs, so only a single copy is mirrored if there is a match within more than one ACL. You can configure the following: ■ Ethertype to be mirrored with the Ethertype ACL mirror option. See "ip access-list eth" on page 208. ■ IP flows to be mirrored with the session ACL mirror option. See "ip access-list session" on page 214. ■ MAC flows to be mirrored with the MAC ACL mirror option. See "ip access-list mac" on page 212. **NOTE:** If you configure both an IP address and a port to receive mirrored packets, the IP address takes precedence.	—	—
ip-address	Configures the IP address of the mirrored destination. Packets are encapsulated in GRE and sent to the destination IP address.		
port	Configures the port of the mirrored destination. Packets are forwarded to the destination port.		
<slot>	<slot> is always 1 except for the OAW-6000 WLAN switch, where the slots can be 0, 1, 2, or 3.	—	—

<port>	Number assigned to the network interface embedded in the WLAN switch or in the line card installed in the OAW-6000 WLAN switch. Port numbers start at 0 from the left-most position.	—	—
session-mirror-ipsec	Configures session mirroring of all frames that are processed by IPSec. Frames are sent to IP address specified by the session-mirror-destination option.This option is used only for troubleshooting or debugging.	—	disabled
session-voip-timeout	Idle session timeout, in seconds, for sessions that are marked as voice sessions. If no voice packet exchange occurs over a voice session for the specified time, the voice session is removed.	16-300	300 seconds
voip-proxy-arp	Reduces the number of broadcast packets sent to VoIP clients, thereby improving the battery life of voice handsets. You can enable this option for voice handsets in conjunction with increasing the DTIM interval on clients. **NOTE:** This parameter is deprecated in all the releases after and including AOS-W 3.3.2. If the voip-proxy-arp command was used in a previous release as a global configuration, it will be disabled after you upgrade to AOS-W 3.3.2. You can now use this option for individual virtual-ap profiles. See the wlan commands section for more information. **NOTE:** Requires voice license.	—	disabled
wmm-voip-content-enforcement	If traffic to or from the user is inconsistent with the associated QoS policy for voice, the traffic is reclassified to best effort and data path counters incremented. **NOTE:** This parameter requires the Voice Services Module license in the WLAN switch.	—	disabled

Usage Guidelines

This command configures global firewall options on the WLAN switch.

Example

The following command disallows forwarding of non-IP frames between users:

```
firewall deny-inter-user-bridging
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for noted parameters.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0. The wmm-voip-content-enforcement parameter was introduced in AOS-W 3.1.

The session-mirror-destination parameter was modified in AOS-W 3.3.

The voip-proxy-arp command has been deprecated in the AOS-W 3.3.2.

The local-valid-users parameter has been added in the AOS-W 3.3.2.

halt

```
halt
```

Description

This command halts all processes on the WLAN switch.

Syntax

No parameters.

Usage Guidelines

This command gracefully stops all processes on the WLAN switch. You should issue this command before rebooting or shutting down to avoid interrupting processes.

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode.

History

This command was available in AOS-W 3.0.

help

```
help
```

Description

This command displays help for the CLI.

Syntax

No parameters.

Usage Guidelines

This command displays keyboard editing commands that allow you to make corrections or changes to the a command without retyping.

You can also enter the question mark (?) to get various types of command help:

- When typed at the beginning of a line, the question mark lists all commands available in the current mode.
- When typed at the end of a command or abbreviation, the question mark lists possible commands that match.
- When typed in place of a parameter, the question mark lists available options.

Example

The following command displays help:

```
help
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in user, enable, and config modes.

History

This command was available in AOS-W 3.0.

hostname

```
hostname <hostname>
```

Description

This command changes the hostname of the WLAN switch.

Syntax

Parameter	Description	Range	Default
`hostname`	The hostname of the WLAN switch.	1–63	See below

Usage Guidelines

The hostname is used as the default prompt.

You can use any alphanumeric character, punctuation, or symbol character. To use spaces, plus symbols (+), question marks (?), or asterisks (*), enclose the text in quotes.

The default names for the following WLAN switches are:

- OmniAccess 4302 WLAN Switch: OAW-4302
- OmniAccess 4308 WLAN Switch: OAW-4308
- OmniAccess 4324 WLAN Switch: OAW-4324
- OmniAccess 4504 WLAN Switch: OAW-4504
- OmniAccess 4604 WLAN Switch: OAW-4604
- OmniAccess 4704 WLAN Switch: OAW-4704
- OmniAccess 6000 WLAN Switch: OAW-6000

Example

The following example configures the WLAN switch hostname to “WLAN switch 1”.

```
hostname “WLAN switch 1”
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 1.0.

ids dos-profile

```
ids dos-profile <profile>
   ap-flood-inc-time <seconds>
   ap-flood-quiet-time <seconds>
   ap-flood-threshold <number>
   assoc-rate-thresholds <number>
   auth-rate-thresholds <number>
   client-ht-40mhz-intol-quiet-time <seconds>
   clone <profile>
   deauth-rate-thresholds <number>
   detect-ap-flood
   detect-disconnect-sta
   detect-eap-rate-anomaly
   detect-ht-40mhz-intolerance
   detect-rate-anomalies
   disassoc-rate-thresholds <number>
   disconnect-sta-quiet-time <seconds>
   eap-rate-quiet-time <seconds>
   eap-rate-threshold <number>
   eap-rate-time-interval <seconds>
   no ...
   probe-request-rate-thresholds <number>
   probe-response-rate-thresholds <number>
   spoofed-deauth-blacklist
```

Description

This command configures traffic anomalies for denial of service (DoS) attacks.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
`ap-flood-inc-time`	Time, in seconds, during which a configured number of fake AP beacons must be received to trigger an alarm.	any	3 seconds
`ap-flood-quiet-time`	After an alarm has been triggered by a fake AP flood, the time, in seconds, that must elapse before an identical alarm may be triggered.	60-360000	900 seconds
`ap-flood-threshold`	Number of fake AP beacons that must be received within the flood increase time to trigger an alarm.	any	50
`assoc-rate-thresholds`	Rate threshold for associate request frames.		
`auth-rate-thresholds`	Rate threshold for authenticate frames.		
`client-ht-40mhz-intol-quiet-time`	Controls the quiet time (when to stop reporting intolerant STAs if they have not been detected), in seconds, for detection of 802.11n 40 MHz intolerance setting.	60-360000	900 seconds
`clone`	Name of an existing IDS DoS profile from which parameter values are copied.	—	—
`deauth-rate-thresholds`	Rate threshold for deauthenticate frames.		
`detect-ap-flood`	Enables detection of flooding with fake AP beacons to confuse legitimate users and to increase the amount of processing needed on client operating systems.	—	disabled

detect-disconnect-sta	Enables detection of station disconnection attacks.	—	disabled
detect-eap-rate-anomaly	Enables Extensible Authentication Protocol (EAP) handshake analysis to detect an abnormal number of authentication procedures on a channel and generate an alarm when this condition is detected.	—	disabled
detect-ht-40mhz-intolerance	Enables or disables detection of 802.11n 40 MHz intolerance setting, which controls whether stations and APs advertising 40 MHz intolerance will be reported.	—	enabled
detect-rate-anomalies	Enables detection of rate anomalies.	—	disabled
disassoc-rate-thresholds	Rate threshold for disassociate frames.		
disconnect-sta-quiet-time	After a station disconnection attack is detected, the time, in seconds, that must elapse before another identical alarm can be generated.	60-360000	900 seconds
eap-rate-quiet-time	After an EAP rate anomaly alarm has been triggered, the time, in seconds, that must elapse before another identical alarm may be triggered.	60-360000	900 seconds
eap-rate-threshold	Number of EAP handshakes that must be received within the EAP rate time interval to trigger an alarm.	any	60
eap-rate-time-interval	Time, in seconds, during which the configured number of EAP handshakes must be received to trigger an alarm.	1-120	3 seconds
no	Negates any configured parameter.	—	—
probe-request-rate-thresholds	Rate threshold for probe request frames.		
probe-response-rate-thresholds	Rate threshold for probe response frames.		
spoofed-deauth-blacklist	Enables detection of a deauth attack initiated against a client associated to an OmniAccess AP. When such an attack is detected, the client is quarantined from the network to prevent a man-in-the-middle attack from being successful.	—	disabled

Usage Guidelines

DoS attacks are designed to prevent or inhibit legitimate clients from accessing the network. This includes blocking network access completely, degrading network service, and increasing processing load on clients and network equipment.

NOTE: AP configuration settings related to the IEEE 802.11n draft standard are configurable for Alcatel-Lucent's OAW-AP120 series access points, which are IEEE 802.11n draft standard compliant devices.

There are four predefined DoS profiles, each of which provides different levels of detection and containment. The following describes the settings for each of the predefined profiles:

Parameter	ids-dos-disabled	ids-dos-low-setting	ids-dos-medium-setting	ids-dos-high-setting
Detect Disconnect Station Attack	disabled	enabled	enabled	enabled
Disconnect STA Detection Quiet Time	900 seconds	900 seconds	900 seconds	900 seconds
Spoofed Deauth Blacklist	disabled	disabled	disabled	disabled
Detect AP Flood Attack	disabled	disabled	disabled	disabled

AP Flood Threshold	50	50	50	50
AP Flood Increase Time	3 seconds	3 seconds	3 seconds	3 seconds
AP Flood Detection Quiet Time	900 seconds	900 seconds	900 seconds	900 seconds
Detect EAP Rate Anomaly	disabled	disabled	enabled	enabled
EAP Rate Threshold	60	60	30	60
EAP Rate Time Interval	3 seconds	3 seconds	3 seconds	3 seconds
EAP Rate Quiet Time	900 seconds	900 seconds	900 seconds	900 seconds
Detect Rate Anomalies	disabled	disabled	disabled	enabled
Detect 802.11n 40 MHz Intolerance Setting	disabled	enabled	enabled	enabled
Client 40 MHz Intolerance Detection Quiet Time	900 seconds	900 seconds	900 seconds	900 seconds
Rate Thresholds for Assoc Frames	default	default	default	default
Rate Thresholds for Disassoc Frames	default	default	default	default
Rate Thresholds for Deauth Frames	default	default	default	default
Rate Thresholds for Probe Request Frames	default	probe-request-response-thresholds	probe-request-response-thresholds	probe-request-response-thresholds
Rate Thresholds for Probe Response Frames	default	probe-request-response-thresholds	probe-request-response-thresholds	probe-request-response-thresholds
Rate Thresholds for Auth Frames	default	default	default	default

Example

The following command enables detections in the DoS profile:

```
ids dos-profile dos1
   detect-ap-flood
   detect-disconnect-sta
   detect-eap-rate-anomalies
   detect-rate-anomalies
   spoofed-deauth-blacklist
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Wireless Intrusion Protection license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

Support for the high-throughput IEEE 802.11n draft standard was introduced in AOS-W 3.3.

ids general-profile

```
ids general-profile <name>
   ap-inactivity-timeout <seconds>
   clone <profile>
   min-pot-ap-beacon-rate <percent>
   min-pot-ap-monitor-time <seconds>
   no ...
   signature-quiet-time <seconds>
   sta-inactivity-timeout <seconds>
   stats-update-interval <seconds>
   wired-containment
   wireless-containment
   wireless-containment-debug
```

Description

This command configures AP attributes.

Syntax

Parameter	Description	Range	Default
<profile>	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	“default”
ap-inactivity-timeout	Time, in seconds, after which an AP is aged out.	5-36000	5 seconds
clone	Name of an existing IDS general profile from which parameter values are copied.	—	—
min-pot-ap-beacon-rate	Minimum beacon rate acceptable from a potential AP, in percentage of the advertised beacon interval.	0-100	25%
min-pot-ap-monitor-time	Minimum time, in seconds, a potential AP has to be up before it is classified as a real AP.	any	2 seconds
no	Negates any configured parameter.	—	—
signature-quiet-time	After a signature match is detected, the time to wait, in seconds, to resume checking.	60-360000	900 seconds
sta-inactivity-timeout	Time, in seconds, after which a station is aged out.	30-360000	60 seconds
stats-update-interval	Interval, in seconds, for the AP to update the WLAN switch with statistics. This setting takes effect only if the OmniVista Mobility Manager is configured. Otherwise, statistics update to the WLAN switch is disabled.	60-360000	60 seconds
wired-containment	Enable containment from the wired side.	—	disabled
wireless-containment	Enable containment from the wireless side.	—	disabled
wireless-containment-debug	Enable debugging of containment from the wireless side.	—	disabled

Usage Guidelines

This command configures general IDS attributes. There are two predefined general IDS profiles, each of which provides different levels of containment. The following describes the settings for each of the predefined profiles:

Parameter	ids-general-disabled	ids-general-high-setting
Stats Update Interval	60 seconds	60 seconds
AP Inactivity Timeout	5 seconds	5 seconds
STA Inactivity Timeout	60 seconds	60 seconds
Min Potential AP Beacon Rate	25%	25%
Min Potential AP Monitor Time	2 seconds	2 seconds
Signature Quiet Time	900 seconds	900 seconds
Wireless Containment	disabled	enabled
Debug Wireless Containment	disabled	disabled
Wired Containment	disabled	enabled

Example

The following command enables containments in the general IDS profile:

```
ids general-profile general1
  wired-containment
  wireless-containment
  wireless-containment-debug
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Wireless Intrusion Protection license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

ids impersonation-profile

```
ids impersonation-profile <name>
  beacon-diff-threshold <percent>
  beacon-inc-wait-time <seconds>
  clone <profile>
  detect-ap-impersonation
  detect-sequence-anomaly
  no ...
  protect-ap-impersonation
  sequence-diff <number>
  sequence-quiet-time <seconds>
  sequence-time-tolerance <milliseconds>
```

Description

This command configures anomalies for impersonation attacks.

Syntax

Parameter	Description	Range	Default
<profile>	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	“default”
beacon-diff-threshold	Percentage increase in beacon rates that triggers an AP impersonation event.	0-100	50%
beacon-inc-wait-time	Time, in seconds, after the beacon difference threshold is crossed before an AP impersonation event is generated.	any	3 seconds
clone	Name of an existing IDS impersonation profile from which parameter values are copied.	—	—
detect-ap-impersonation	Enables detection of AP impersonation. In AP impersonation attacks, the attacker sets up an AP that assumes the BSSID and ESSID of a valid AP. AP impersonation attacks can be done for man-in-the-middle attacks, a rogue AP attempting to bypass detection, or a honeypot attack.	—	disabled
detect-sequence-anomaly	Enables detection of anomalies between sequence numbers seen in 802.11 frames. During an impersonation attack, the attacker may spoof the MAC address of a client or AP. If two devices are active on the network with the same MAC address, the sequence numbers in the frames will not match since the sequence number is generated by NIC firmware.	—	disabled
no	Negates any configured parameter.	—	—
protect-ap-impersonation	When AP impersonation is detected, both the legitimate and impersonating AP are disabled using a denial of service attack.	—	disabled
sequence-diff	Maximum allowable tolerance between sequence numbers within the sequence number time tolerance period.	any	300
sequence-quiet-time	After a sequence number anomaly alarm has been triggered, the time, in seconds, that must elapse before another identical alarm may be triggered.	60-360000	900 seconds.
sequence-time-tolerance	Time, in seconds, during which sequence numbers must exceed the sequence number difference value for an alarm to be triggered.	any	300 seconds

Usage Guidelines

A successful man-in-the-middle attack will insert an attacker into the data path between the client and the AP. In such a position, the attacker can delete, add, or modify data, provided he has access to the encryption keys. Such an attack also enables other attacks that can learn a client's authentication credentials. Man-in-the-middle attacks often rely on a number of different vulnerabilities.

There are two predefined IDS impersonation profiles, each of which provides different levels of detection. The following describes the settings for each of the predefined profiles:

Parameter	ids-impersonation-disabled	ids-impersonation-high-setting
Detect AP Impersonation	disabled	enabled
Protect from AP Impersonation	disabled	enabled
Beacon Diff Threshold	50%	50%
Beacon Increase Wait Time	3 seconds	3 seconds
Detect Sequence Anomaly	disabled	enabled
Sequence Number Difference	300	300
Sequence Number Time Tolerance	300 milliseconds	300 milliseconds
Sequence Number Quiet Time	900 seconds	900 seconds

Example

The following command enables detections in the impersonation profile:

```
ids impersonation-profile mitm1
   detect-ap-impersonation
   detect-sequence-anomalies
   protect-ap-impersonation
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Wireless Intrusion Protection license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

ids profile

```
ids profile <name>
  clone <profile>
  dos-profile <profile>
  general-profile <profile>
  impersonation-profile <profile>
  no ...
  signature-matching-profile <profile>
  unauthorized-device-profile <profile>
```

Description

This command defines a set of IDS profiles.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
`clone`	Name of an existing IDS profile from which parameter values are copied.	—	—
`dos-profile`	Name of a IDS denial of service profile to be applied to the AP group/name. See "ids dos-profile" on page 174.	—	"default"
`general-profile`	Name of an IDS general profile to be applied to the AP group/name. See "ids general-profile" on page 177.	—	"default"
`impersonation-profile`	Name of an IDS impersonation profile to be applied to the AP group/name. See "ids impersonation-profile" on page 179.	—	"default"
`no`	Negates any configured parameter.	—	—
`signature-matching-profile`	Name of an IDS signature matching profile to be applied to the AP group/name. See "ids signature-matching-profile" on page 185	—	"default"
`unauthorized-device-profile`	Name of an IDS unauthorized device profile to be applied to the AP group/name. See "ids unauthorized-device-profile" on page 189.	—	"default"

Usage Guidelines

This command defines a set of IDS profiles that you can then apply to an AP group (with the **ap-group** command) or to a specific AP (with the **ap-name** command).

There are four predefined IDS profiles, each of which defines different sets of IDS profile. The following describes the settings for each of the predefined profiles:

Parameter	ids-disabled	ids-low-setting	ids-medium-setting	ids-high-setting
IDS General profile	ids-general-disabled	default	default	ids-general-high-setting
IDS Signature Matching profile	default	factory-default-signatures	factory-default-signatures	factory-default-signatures
IDS DoS profile	ids-dos-disabled	ids-dos-low-setting	ids-dos-medium-setting	ids-dos-high-setting
IDS Impersonation profile	ids-impersonation-disabled	default	default	ids-impersonation-high-setting

IDS Unauthorized Device profile	ids-unauthorized-device-disabled	default	ids-unauthorized-device-medium-setting	ids-unauthorized-device-high-setting

Example

The following command defines a set of IDS profiles:

```
ids profile ids1
   dos-profile dos1
   general-profile general1
   impersonation-profile mitm1
   signature-matching-profile sig1
   unauthorized-device-profile unauth1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Wireless Intrusion Protection license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

ids rate-thresholds-profile

```
ids rate-thresholds-profile <name>
  channel-inc-time <seconds>
  channel-quiet-time <seconds>
  clone <profile>
  no ...
  node-quiet-time <seconds>
  node-threshold <number>
  node-time-interval <seconds>
```

Description

This command configures thresholds that are assigned to the different frame types for rate anomaly checking.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
`channel-inc-time`	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.	any	15 seconds
`channel-quiet-time`	After a channel rate anomaly alarm has been triggered, the time that must elapse before another identical alarm may be triggered. This option prevents excessive messages in the log file.	60-360000	900 seconds
`channel-threshold`	Number of a specific type of frame that must be exceeded within a specific interval in an entire channel to trigger an alarm.	any	300
`clone`	Name of an existing IDS rate thresholds profile from which parameter values are copied.	—	—
`no`	Negates any configured parameter.	—	—
`node-quiet-time`	After a node rate anomaly alarm has been triggered, the time, in seconds, that must elapse before another identical alarm may be triggered. This option prevents excessive messages in the log file.	60-360000	900 seconds
`node-threshold`	Number of a specific type of frame that must be exceeded within a specific interval for a particular client MAC address to trigger an alarm.	any	200
`node-time-interval`	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.	1-120	15 seconds

Usage Guidelines

A profile of this type is attached to each of the following 802.11 frame types in the IDS denial of service profile:

- Association frames
- Disassociation frames
- Deauthentication frames
- Probe Request frames
- Probe Response frames
- Authentication frames

There is a predefined IDS rate thresholds profile. The following describes the settings for the predefined profile:

Parameter	probe-request-response-thresholds
Channel Increase Time	30 seconds
Channel Quiet Time	900 seconds
Channel Threshold	350
Node Time Interval	10 seconds
Node Quiet Time	900 seconds
Node Threshold	250 seconds

Example

The following command configures frame thresholds:

```
ids rate-thresholds-profile rate1
   channel-threshold 250
   node-threshold 150
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Wireless Intrusion Protection license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

ids signature-matching-profile

```
ids signature-matching-profile <name>
  clone <profile>
  no ...
  signature <profile>
```

Description

This command contains defined signature profiles.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
`clone`	Name of an existing IDS signature matching profile from which parameter values are copied.	—	—
`no`	Negates any configured parameter.	—	—
`signature`	Name of a signature profile. See "ids signature-profile" on page 187.	—	—

Usage Guidelines

You can include one or more predefined signature profiles or a user-defined signature profile in a signature matching profile. The following are predefined signature profiles that are included in the signature matching profile called "factory-default-signatures":

Signature	Description
AirJack	Originally a suite of device drivers for 802.11(a/b/g) raw frame injection and reception. It was intended to be used as a development tool for all 802.11 applications that need to access the raw protocol, however one of the tools included allowed users to force off all users on an Access Point.
ASLEAP	A tool created for Linux systems that has been used to attack Cisco LEAP authentication protocol.
Deauth-Broadcast	A deauth broadcast attempts to disconnect all stations in range – rather than sending a spoofed deauth to a specific MAC address, this attack sends the frame to a broadcast address.
NetStumbler Generic	NetStumbler is a popular wardriving application used to locate 802.11 networks. When used with certain NICs (such as Orinoco), NetStumbler generates a characteristic frame that can be detected.
NetStumbler Version 3.3.0x	Version 3.3.0 of NetStumbler changed the characteristic frame slightly. This signature detects the updated frame.
Null-Probe-Response	An attack with the potential to crash or lock up the firmware of many 802.11 NICs. In this attack, a client probe-request frame will be answered by a probe response containing a null SSID. A number of popular NIC cards will lock up upon receiving such a probe response.

Example

The following command configures a signature matching profile:

```
ids signature-matching-profile sig1
   signature Null-Probe-Response
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Wireless Intrusion Protection license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

ids signature-profile

```
ids signature-profile <name>
   bssid <macaddr>
   clone <profile>
   dst-mac <macaddr>
   frame-type {assoc|auth|beacon|control|data|deauth|disassoc|mgmt|probe-request|
    probe-response} [ssid <ssid>] [ssid-length <bytes>]
   no ...
   payload <pattern> [offset <number>]
   seq-num <number>
   src-mac <macaddr>
```

Description

This command configures signatures for wireless intrusion detection.

Syntax

Parameter	Description	Range	Default
<profile>	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
bssid	BSSID field in the 802.11 frame header.	—	—
clone	Name of an existing IDS signature profile from which parameter values are copied.	—	—
dst-mac	Destination MAC address in the 802.11 frame header.	—	—
frame-type	Type of 802.11 frame. For each type of frame, further parameters can be specified to filter and detect only the required frames.	—	—
assoc	Association frame type		
auth	Authentication frame type		
beacon	Beacon frame type		
control	All control frames		
data	All data frames		
deauth	Deauthentication frame type		
disassoc	Disassociation frame type		
mgmt	Management frame type		
probe-re quest	Probe request frame type		
probe-re sponse	Probe response frame type		
ssid	For beacon, probe-request, and probe-response frame types, specify the SSID as either a string or hex pattern.	—	—
ssid-length	For beacon, probe-request, and probe-response frame types, specify the length, in bytes, of the SSID. Maximum length is 32 bytes.	—	—
no	Negates any configured parameter.	—	—
payload	Pattern at a fixed offset in the payload of an 802.11 frame. Specify the pattern to be matched as a string or hex pattern. Maximum length is 32 bytes.	—	—

offset	When a payload pattern is configured, specify the offset in the payload where the pattern is expected to be found in the frame.	—	—
seq-num	Sequence number of the frame.	—	—
src-mac	Source MAC address in the 802.11 frame header.	—	—

Usage Guidelines

The following describes the configuration for the predefined signature profiles:

Signature Profile	Parameter	Value
AirJack	frame-type	beacon ssid = AirJack
ASLEAP	frame-type	beacon ssid = asleap
Deauth-Broadcast	frame-type	deauth
	dst-mac	ff:ff:ff:ff:ff:ff
Netstumbler Generic	payload	offset=3 pattern=0x00601d
	payload	offset=6 pattern=0x0001
Netstumbler Version 3.3.0x	payload	offset=3 pattern=0x00601d
	payload	offset=12 pattern=0x000102
Null-Probe-Response	frame-type	probe-response ssid length = 0

Example

The following command configures a signature profile:

```
ids signature-profile mysig
  frame-type assoc
  src-mac 00:00:00:00:00:00
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Wireless Intrusion Protection license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

ids unauthorized-device-profile

```
ids unauthorized-device-profile <name>
  adhoc-quiet-time <seconds>
  allow-well-known-mac [hsrp|iana|local-mac|vmware|vmware1|vmware2|vmware3]
  cfg-valid-11a-channel <channel>
  cfg-valid-11g-channel <channel>
  classification
  clone <profile>
  detect-adhoc-network
  detect-bad-wep
  detect-ht-greenfield
  detect-invalid-mac-oui
  detect-misconfigured-ap
  detect-windows-bridge
  detect-wireless-bridge
  mac-oui-quiet-time <seconds>
  no ...
  overlay-classification
  privacy
  protect-adhoc-network
  protect-high-throughput
  protect-ht-40mhz
  protect-misconfigured-ap
  protect-ssid
  protect-valid-sta
  require-wpa
  rogue-containment
  suspect-rogue-conf-level <level>
  suspect-rogue-containment
  valid-and-protected-ssid <ssid>
  valid-oui <oui>
  valid-wired-mac <macaddr>
  wireless-bridge-quiet-time <seconds>
```

Description

This command configures detection of unauthorized devices, as well as rogue AP detection and containment.

Syntax

Parameter	Description	Range	Default
<profile>	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	“default”
adhoc-quiet-time	Time, in seconds, that must elapse after an adhoc network detection alarm has been triggered before another identical alarm may be triggered.	60-360000	900 seconds

`allow-well-known-mac`	Allows devices with known MAC addresses to classify rogues APs. Depending on your network, configure one or more of the following options for classifying rogue APs: ■ hsrp—Routers configured for HSRP, a Cisco-proprietary redundancy protocol, with the HSRP MAC OUI 00:00:0c. ■ iana—Routers using the IANA MAC OUI 00:00:5e. ■ local-mac—Devices with locally administered MAC addresses starting with 02. ■ vmware—Devices with any of the following VMWare OUIs: 00:0c:29, 00:05:69, or 00:50:56 ■ vmware1—Devices with VMWare OUI 00:0c:29. ■ vmware2—Devices with VMWare OUI 00:05:69. ■ vmware3—Devices with VMWare OUI 00:50:56. If you modify an existing configuration, the new configuration overrides the original configuration. For example, if you configure `allow-well-known-mac hsrp` and then configure `allow-well-known-mac iana`, the original configuration is lost. To add more options to the original configuration, include all of the required options, for example: `allow-well-known-mac hsrp iana`. **NOTE:** Use caution when configuring this command. If the neighboring network uses similar routers, those APs might be classified as rogues. If containment is enabled, clients attempting to associate to an AP classified as a rogue are disconnected through a denial of service attack. To clear the well known MACs in the system, use the following commands on all WLAN switches: **1.** `clear wms wired-mac` This clears all of the learned wired MAC information on the WLAN switch. **2.** `reload` This reboots the WLAN switch.	—	—
`cfg-valid-11a-channel`	List of valid 802.11a channels that third-party APs are allowed to use.	34-165	36, 44, 52, 60, 40, 48, 56, 64
`cfg-valid-11g-channel`	List of valid 802.11b/g channels that third-party APs are allowed to use.	1-14	1, 6, 11
`classification`	Enable/disable rogue AP classification. A rogue AP is one that is unauthorized and plugged into the wired side of the network. Any other AP seen in the RF environment that is not part of the valid enterprise network is considered to be interfering — it has the potential to cause RF interference but it is not connected to the wired network and thus does not represent a direct threat.	—	enabled
`clone`	Name of an existing IDS rate thresholds profile from which parameter values are copied.	—	—
`detect-adhoc-network`	Enable detection of adhoc networks.	—	disabled
`detect-bad-wep`	Enables detection of WEP initialization vectors that are known to be weak and/or repeating. A primary means of cracking WEP keys is to capture 802.11 frames over an extended period of time and search for implementations that are still used by many legacy devices.	—	disabled

detect-ht-greenfield	Enables or disables detection of high-throughput devices advertising greenfield preamble capability.	—	enabled
detect-invalid-mac-oui	Enables checking of the first three bytes of a MAC address, known as the organizationally unique identifier (OUI), assigned by the IEEE to known manufacturers. Often clients using a spoofed MAC address do not use a valid OUI and instead use a randomly generated MAC address. Enabling MAC OUI checking causes an alarm to be triggered if an unrecognized MAC address is in use.	—	disabled
detect-misconfigured-ap	Enables detection of misconfigured APs. An AP is classified as misconfigured if it is classified as valid and does not meet any of the following configurable parameters: - valid channels - encryption type - list of valid AP MAC OUIs - valid SSID list	—	disabled
detect-windows-bridge	Enables detection of Windows station bridging.	—	disabled
detect-wireless-bridge	Enables detection of wireless bridging.	—	disabled
mac-oui-quiet-time	Time, in seconds, that must elapse after an invalid MAC OUI alarm has been triggered before another identical alarm may be triggered.		900 seconds
no	Negates any configured parameter.	—	—
overlay-classification	This option is useful when OmniAccess APs are used for monitoring a non-OmniAccess wireless network, as it allows APs that are plugged into the wired side of the network to be classified as “suspected rogue” instead of “rogue”. Suspected rogue APs are not subject to the rogue containment settings; however, if configured, they are subject to the suspected rogue AP containment settings (see suspect-rogue-containment).	—	enabled
privacy	Enables encryption as a valid AP configuration.	—	disabled
protect-adhoc-network	Enables protection from adhoc networks. When adhoc networks are detected, they are disabled using a denial of service attack.	—	disabled
protect-high-throughput	Enables or disables protection of high-throughput (802.11n) devices.	—	disabled
protect-ht-40mhz	Enables or disables protection of high-throughput (802.11n) devices operating in 40 MHz mode.	—	disabled
protect-misconfigured-ap	Enables protection of misconfigured APs.	—	disabled
protect-ssid	Enables use of SSID by valid APs only.	—	disabled
protect-valid-sta	When enabled, does not allow valid stations to connect to a non-valid AP.	—	disabled
require-wpa	When enabled, any valid AP that is not using WPA encryption is flagged as misconfigured.	—	disabled
rogue-containment	Rogue APs can be detected (see classification) but are not automatically disabled. This option automatically shuts down rogue APs. When this option is enabled, clients attempting to associate to an AP classified as a rogue are disconnected through a denial of service attack.	—	disabled

suspect-rogue-conf-level	Confidence level of suspected Rogue AP to trigger containment. When an AP is classified as a suspected rogue AP, it is assigned a 50% confidence level. If multiple APs trigger the same events that classify the AP as a suspected rogue, the confidence level increases by 5% up to 95%. In combination with suspected rogue containment, this option configures the threshold by which containment should occur. Suspected rogue containment occurs only when the configured confidence level is met.	50-100	60%
suspect-rogue-containment	Suspected rogue APs are treated as interfering APs, thereby the WLAN switch attempts to reclassify them as rogue APs. Suspected rogue APs are not automatically contained. In combination with the configured confidence level (see suspect-rogue-conf-level), this option contains the suspected rogue APs.	—	disabled
valid-and-protected-ssid	List of valid and protected SSIDs.	—	—
valid-oui	List of valid MAC OUIs.	—	—
valid-wired-mac	List of MAC addresses of wired devices in the network, typically gateways or servers.	—	—
wireless-bridge-quiet-time	Time, in seconds, that must elapse after a wireless bridge alarm has been triggered before another identical alarm may be triggered.	60-360000	900 seconds

Usage Guidelines

Unauthorized device detection includes the ability to detect and disable rogue APs and other devices that can potentially disrupt network operations.

NOTE: AP configuration settings related to the IEEE 802.11n draft standard are configurable for Alcatel-Lucent's OAW-AP120 series access points, which are IEEE 802.11n draft standard compliant devices.

There are three predefined unauthorized device profiles, each of which provides different levels of detection and containment. The following describes the settings for each of the predefined profiles:

Parameter	ids-unauthorized-device-disabled	ids-unauthorized-device-medium-setting	ids-unauthorized-device-high-setting
Detect adhoc networks	disabled	enabled	enabled
Protect from adhoc networks	disabled	disabled	enabled
Detect windows bridge	disabled	enabled	enabled
Detect wireless bridge	disabled	enabled	enabled
Detect devices with invalid MAC OUI	disabled	disabled	enabled
MAC OUI detection quiet time	900 seconds	900 seconds	900 seconds
Adhoc network detection quiet time	900 seconds	900 seconds	900 seconds
Wireless bridge detection quiet time	900 seconds	900 seconds	900 seconds
Rogue AP classification	disabled	enabled	enabled
Overlay rogue AP classification	enabled	enabled	enabled
Valid wired MACs	—	—	—
Rogue containment	disabled	disabled	enabled

Allow well known MAC	—	—	—
Suspected rogue containment	disabled	disabled	disabled
Suspected rogue containment confidence level	60	60	60
Protect valid stations	disabled	disabled	enabled
Detect bad WEP	disabled	enabled	enabled
Detect misconfigured AP	disabled	enabled	enabled
Protect misconfigured AP	disabled	disabled	enabled
Protect SSID	disabled	disabled	enabled
Privacy	disabled	disabled	enabled
Require WPA	disabled	enabled	disabled
Valid 802.11g channel for policy enforcement	—	—	—
Valid 802.11a channel for policy enforcement	—	—	—
Valid MAC OUIs	—	—	—
Valid and protected SSIDs	—	—	—
Protect 802.11n High-throughput Devices	disabled	disabled	enabled
Protect 40 MHz 802.11n High-throughput Devices	disabled	disabled	enabled
Detect Active 802.11n Greenfield Mode	disabled	enabled	enabled

Example

The following command copies the settings from the ids-unauthorized-device-disabled profile and then enables detection and protection from adhoc networks:

```
ids unauthorized-device-profile unauth1
   clone ids-unauthorized-device-disabled
   detect-adhoc-network
   protect-adhoc-network
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Wireless Intrusion Protection license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

Support for the high-throughput IEEE 802.11n draft standard was introduced in AOS-W 3.3. The allow-well-known-mac, suspect-rogue-conf-level, and suspect-rogue-containment parameters were also introduced in AOS-W 3.3.

interface fastethernet | gigabitethernet

```
interface {fastethernet|gigabitethernet} <slot>/<port>
  description <string>
  duplex {auto|full|half}
  ip access-group <acl> {in|out|session}
  muxport
  no ...
  poe [cisco]
  port monitor {fastethernet|gigabitethernet} <slot>/<port>
  priority-map <name>
  shutdown
  spanning-tree [cost <value>] [port-priority <value>] [portfast]
  speed {10|100|auto}
  switchport {access vlan <vlan>|mode {access|trunk}|
   trunk {allowed vlan {<vlans>|add <vlans>|all|except <vlans>|remove <vlans>}|
   native vlan <vlan>}}
  trusted
  xsec {point-to-point <macaddr> <key> allowed vlan <vlans> [<mtu>]|vlan <vlan>}
```

Description

This command configures a FastEthernet or GigabitEthernet interface on the WLAN switch.

Syntax

Parameter	Description	Range	Default
<slot>	<slot> is always 1 except for the OAW-6000 WLAN switch, where the slots can be 0, 1, 2, or 3.	—	—
<port>	Number assigned to the network interface embedded in the WLAN switch, or for the OAW-6000 WLAN switch, in a line card or the Multi-Service Mobility Module Mark I. Port numbers start at 0 from the left-most position.	—	—
description	String that describes this interface.	—	—
duplex	Transmission mode on the interface: full- or half-duplex or auto to automatically adjust transmission.	auto/full/half	auto
ip access-group	Applies the specified access control list (ACL) to the interface. Use the **ip access-list** command to configure an ACL. **NOTE**: The Policy Enforcement Firewall license must be installed.	—	—
in	Apply ACL to interface's inbound traffic.	—	—
out	Apply ACL to interface's outbound traffic.	—	—
session	Apply session ACL to interface.	—	—
muxport	Enable MUX capability on the interface.	—	disabled
no	Negates any configured parameter.	—	—
poe	Enables Power-over-Ethernet (PoE) on the interface.	—	enabled
cisco	Enables Cisco-style PoE on the interface.	—	disabled
port monitor	Monitors another interface on the WLAN switch.	—	—
priority-map	Applies a priority map to the interface. Use the **priority-map** command to configure a priority map which allows you to map ToS and CoS values into high priority traffic queues.	—	—

shutdown	Causes a hard shutdown of the interface.	—	—
spanning-tree	Enables spanning tree.	—	enabled
cost	Administrative cost associated with the spanning tree.	1-65535	19 (Fast Ethernet) 4 (Gigabit Ethernet)
port-priority	Spanning tree priority of the interface. A lower setting brings the port closer to root port position (favorable for forwarding traffic) than does a higher setting. This is useful if ports may contend for root position if they are connected to an identical bridge.	0-255	128
portfast	Enables forwarding of traffic from the interface.	—	disabled
speed	Sets the interface speed: 10 Mbps, 100 Mbps, or auto configuration.	10|100|auto	auto
switchport	Sets switching mode parameters for the interface.	—	—
access vlan	Sets the interface as an access port for the specified VLAN. The interface carries traffic only for the specified VLAN.	—	1
mode	Sets the mode of the interface to access or trunk mode only.	access|trunk	access
trunk	Sets the interface as a trunk port for the specified VLANs. A trunk port carries traffic for multiple VLANs using 802.1q tagging to mark frames for specific VLANs. You can include all VLANs configured on the WLAN switch, or add or remove specified VLANs. Specify **native** to identify the native VLAN for the trunk mode interface. Frames on the native VLAN are not 802.1q tagged.	—	—
trusted	Set this interface to be trusted. Trusted ports are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When OmniAccess APs are attached directly to the WLAN switch, set the port to be trusted.	—	disabled
xsec	Enables and configures the Extreme Security (xSec) protocol. **NOTE**: You must purchase and install the xSec software module license in the WLAN switch.	—	—
point-to-point	MAC address of the WLAN switch that is the xSec tunnel termination point, and the 16-byte shared key used to authenticate the WLAN switches to each other. The key must be the same on both WLAN switches.	—	—
allowed vlan	VLANs that are allowed on the xSec tunnel.	—	—
mtu	(Optional) MTU size for the xSec tunnel.	—	—
vlan	xSec VLAN ID. For WLAN switch-to-WLAN switch communications, both WLAN switches must belong to the same VLAN.	1-4094	—

Usage Guidelines

Use the **show port status** command to obtain information about the interfaces available on the WLAN switch.

Example

The following command configures an interface as a trunk port for a set of VLANs:

```
interface fastethernet 1/22
   switchport mode trunk
   switchport trunk native vlan 10
   switchport trunk allowed vlan 1,10,100
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system. The **ip access-group** parameter requires the PEF license. The **xsec** parameter requires the xSec license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

interface loopback

```
interface loopback
  ip address <ipaddr>
  no ...
```

Description

This command configures the loopback address on the WLAN switch.

Syntax

Parameter	Description	Range	Default
`ip address`	Host address with a 32-bit netmask. This address should be routable from all external networks.	—	—
`no`	Negates any configured parameter.	—	—

Usage Guidelines

If configured, the loopback address is used as the WLAN switch's IP address. If you do not configure a loopback address for the WLAN switch, the IP address assigned to VLAN 1 is used as the WLAN switch's IP address.

NOTE: After you configure or modify a loopback address, you need to reboot the WLAN switch.

Example

The following command configures a loopback address:

```
interface loopback
  ip address 10.2.22.220
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

interface mgmt

```
interface mgmt
  dhcp
  ip address <ipaddr> <netmask>
  no ...
  shutdown
```

Description

This command configures the out-of-band Ethernet management port on an OmniAccess 6000 WLAN switch.

Syntax

Parameter	Description	Range	Default
`dhcp`	Enables DHCP on the interface.	—	—
`ip address`	Configures an IP address and netmask on the interface.	—	—
`no`	Negates any configured parameter.	—	—
`shutdown`	Causes a hard shutdown of the interface.	—	—

Usage Guidelines

This command applies to OmniAccess Supervisor Cards: OmniAccess Supervisor Card I or II (earlier generation supervisor cards, referred to as OAW-SC), and OmniAccess Supervisor Card III (referred to as OAW-S3).

Use the **show interface mgmt** command to view the current status of the management port.

Example

The following command configures an IP address on the management interface:

```
interface mgmt
  ip address 10.1.1.1 255.255.255.0
```

Platform Availability

This command is only available on the OmniAccess 6000 WLAN switch.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

interface port-channel

```
interface port-channel <id>
  add {fastethernet|gigabitethernet} <slot>/<port>
  del {fastethernet|gigabitethernet} <slot>/<port>
  ip access-group <acl> {in|out|session}
  no ...
  shutdown
  spanning-tree [portfast]
  switchport {access vlan <vlan>|mode {access|trunk}|
   trunk {allowed vlan {<vlans>|add <vlans>|all|except <vlans>|remove <vlans>|
   native vlan <vlan>}
  trusted
  xsec {point-to-point <macaddr> <key> allowed vlan <vlans> [<mtu>]|vlan <vlan>}
```

Description

This command configures an Ethernet port channel.

Syntax

Parameter	Description	Range	Default
`port-channel`	ID number for this port channel.	0-7	—
`add`	Adds the specified FastEthernet or GigabitEthernet interface to the port channel. **NOTE:** You cannot specify both FastEthernet and GigabitEthernet interfaces for the same port channel.	—	—
`del`	Deletes the specified Fastethernet or Gigabitethernet interface to the port channel.	—	—
`ip access-group`	Applies the specified access control list (ACL) to the interface. Use the **ip access-list** command to configure an ACL. **NOTE**: The Policy Enforcement Firewall license must be installed.	—	—
`in`	Applies ACL to interface's inbound traffic.	—	—
`out`	Applies ACL to interface's outbound traffic.	—	—
`session`	Applies session ACL to interface.	—	—
`no`	Negates any configured parameter.	—	—
`shutdown`	Causes a hard shutdown of the interface.	—	—
`spanning-tree`	Enables spanning tree.	—	—
`portfast`	Enables forwarding of traffic from the interface.	—	—
`switchport`	Sets switching mode parameters for the interface.	—	—
`access vlan`	Sets the interface as an access port for the specified VLAN. The interface carries traffic only for the specified VLAN.	—	—
`mode`	Sets the mode of the interface to access or trunk mode only.	—	—
`trunk`	Sets the interface as a trunk port for the specified VLANs. A trunk port carries traffic for multiple VLANs using 802.1q tagging to mark frames for specific VLANs. You can include all VLANs configured on the WLAN switch, or add or remove specified VLANs.	—	—

native	Specifies the native VLAN for the trunk mode interface. Frames on the native VLAN are not 802.1q tagged.	—	—
trusted	Set this interface to be trusted. Trusted ports are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When OmniAccess APs are attached directly to the WLAN switch, set the port to be trusted.	—	disabled
xsec	Enables and configures the Extreme Security (xSec) protocol. **NOTE**: You must purchase and install the xSec software module license in the WLAN switch.	—	—
point-to-point	MAC address of the WLAN switch that is the xSec tunnel termination point, and the 16-byte shared key used to authenticate the WLAN switches to each other. The key must be the same on both WLAN switches.	—	—
allowed vlan	VLANs that are allowed on the xSec tunnel.	—	—
mtu	(Optional) MTU size for the xSec tunnel.	—	—
vlan	xSec VLAN ID. For WLAN switch-to-WLAN switch communications, both WLAN switches must belong to the same VLAN.	1-4094	—

Usage Guidelines

A port channel allows you to aggregate ports on a WLAN switch. You can configure a maximum of 8 port channels per supported WLAN switch with a maximum of 16 interfaces per port channel.

NOTE: A port channel does *not* use the Link Aggregation Control Protocol (LACP), which is part of the IEEE 802.3ad specification.

Note the following when setting up a port channel between a WLAN switch and a Cisco switch (such as a Catalyst 6500 Series Switch):

- There must be no negotiation of the link parameters.
- The configuration on the Cisco switch must not include LACP.
- The port-channel mode on the Cisco switch must be “on”.

Example

The following command configures a port channel:

```
interface port channel 7
  add fastethernet 1/1
  add fastethernet 1/2
```

Platform Availability

This command is available only on OmniAccess 4324, 4504, 4604, 4704, and 6000 WLAN switches.

Licensing Requirements

This command is available in the base operating system. The **ip access-group** parameter requires the PEF license. The **xsec** parameter requires the xSec license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

interface range

```
interface range {fastethernet|gigabitethernet} <slot>/<port>-<port>
  duplex {auto|full|half}
  ip access-group <acl> {in|out|session}
  no ...
  poe [cisco]
  shutdown
  spanning-tree [cost <value>] [port-priority <value>] [portfast]
  speed {10|100|auto}
  switchport {access vlan <vlan>|mode {access|trunk}|
   trunk {allowed vlan {<vlans>|add <vlans>|all|except <vlans>|remove <vlans>}|
   native vlan <vlan>}}
  trusted
```

Description

This command configures a range of FastEthernet or GigabitEthernet interfaces on the WLAN switch.

Syntax

Parameter	Description	Range	Default
range	Range of Ethernet ports in the format <slot>/<port>-<port>.	—	—
duplex	Transmission mode on the interface: full- or half-duplex or auto to automatically adjust transmission.	auto/full/half	auto
ip access-group	Applies the specified access control list (ACL) to the interface. Use the ip access-list command to configure an ACL.	—	—
in	Apply ACL to interface's inbound traffic.	—	—
out	Apply ACL to interface's outbound traffic.	—	—
session	Apply session ACL to interface.	—	—
no	Negates any configured parameter.	—	—
poe	Enables Power-over-Ethernet (PoE) on the interface.	—	—
cisco	Enables Cisco-style PoE on the interface.	—	—
shutdown	Causes a hard shutdown of the interface.	—	—
spanning-tree	Enables spanning tree.	—	—
cost	Administrative cost associated with the spanning tree.	1-65535	—
port-priority	Spanning tree priority of the interface. A lower setting brings the port closer to root port position (favorable for forwarding traffic) than does a higher setting. This is useful if ports may contend for root position if they are connected to an identical bridge.	0-255	
portfast	Enables forwarding of traffic from the interface.	—	—
speed	Sets the interface speed: 10 Mbps, 100 Mbps, or auto configuration.	10l100lauto	auto
switchport	Sets switching mode parameters for the interface.	—	—
access vlan	Sets the interface as an access port for the specified VLAN. The interface carries traffic only for the specified VLAN.	—	—

`mode`	Sets the mode of the interface to access or trunk mode only.	—	—
`trunk`	Sets the interface as a trunk port for the specified VLANs. A trunk port carries traffic for multiple VLANs using 802.1q tagging to mark frames for specific VLANs. You can include all VLANs configured on the WLAN switch, or add or remove specified VLANs. Specify **native** to identify the native VLAN for the trunk mode interface. Frames on the native VLAN are not 802.1q tagged.	—	—
`trusted`	Set this interface to be trusted. Trusted ports are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When OmniAccess APs are attached directly to the WLAN switch, set the port to be trusted.	—	disabled

Usage Guidelines

Use the show port status command to obtain information about the interfaces available on the WLAN switch.

Example

The following command configures a range of interface as a trunk port for a set of VLANs:

```
interface range fastethernet 1/12-15
   switchport mode trunk
   switchport trunk native vlan 10
   switchport trunk allowed vlan 1,10,100
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

interface tunnel

```
interface tunnel <number>
  description <string>
  inter-tunnel-flooding
  ip address <ipaddr> <netmask>
  mtu <mtu>
  no ...
  shutdown
  trusted
  tunnel checksum|destination <ipaddr>|keepalive [<interval> <retries>]|key <key>|
   mode gre {<protocol>|ip}|source {<ipaddr>|loopback|vlan <vlan>}|vlan <vlans>
```

Description

This command configures a tunnel interface.

Syntax

Parameter	Description	Range	Default
`tunnel`	Identification number for the tunnel.	1-2147483647	—
`description`	String that describes this interface.	—	Tunnel Interface
`inter-tunnel-flooding`	Enables inter-tunnel flooding.	—	enabled
`ip address`	IP address of the tunnel. This represents the entrance to the tunnel.	—	—
`mtu`	MTU size for the interface.	—	1500
`no`	Negates any configured parameter.	—	—
`shutdown`	Causes a hard shutdown of the interface.	—	—
`trusted`	Set this interface to be trusted. Trusted ports are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When OmniAccess APs are attached directly to the WLAN switch, set the port to be trusted.	—	disabled
`tunnel`	Configures tunneling.	—	mode gre ip
`checksum`	Enables end-to-end checksum of packets that pass through the tunnel.	—	disabled
`destination`	Destination IP address for the tunnel endpoint.	—	—
`keepalive`	Enables sending of periodic keepalive frames on the tunnel to determine the tunnel status (up or down). You can optionally set the interval at which keepalive frames are sent, and the number of times the frames are resent before a tunnel is considered to be down.	—	disabled
`<interval>`	(Optional) Number of seconds at which keepalive frames are sent.	1-86400	10 seconds
`<retries>`	(Optional) Number of consecutive times that the keepalives fail before the tunnel is considered to be down.	0-1024	3
`key`	Key used to authenticate packets on the tunnel.	0-4294967295	—

`mode gre`	Specifies generic route encapsulation (GRE) type. You configure either a 16-bit protocol number (for Layer-2 tunnels) or **ip** (for a Layer-3 tunnel). The 16-bit protocol number uniquely identifies a Layer-2 tunnel. The WLAN switches at both endpoints of the tunnel must be configured with the same protocol number.	—	—
`source`	The local endpoint of the tunnel on the WLAN switch. This can be one of the following: ■ specified IP address ■ the loopback interface configured on the WLAN switch ■ specified VLAN	—	—
`vlan`	VLANs to be included in this tunnel.	—	—

Usage Guidelines

You can configure a GRE tunnel between an OmniAccess WLAN switch and another GRE-capable device. Layer-3 GRE tunnel type is the default (**tunnel mode gre ip**). You can direct traffic into the tunnel using a static route (specify the tunnel as the next hop for a static route) or a session-based access control list (ACL).

Example

The following command configures a tunnel interface:

```
interface tunnel 200
   ip address 10.1.1.1 255.255.2550
   tunnel source loopback
   tunnel destination 20.1.1.242
   tunnel mode gre ip
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0. The tunnel keepalive parameter was introduced in AOS-W 3.2.

interface vlan

```
interface vlan <vlan>
  bandwidth-contract <name>
  description <string>
  ip address {<ipaddr> <netmask>|dhcp-client|pppoe}|
   helper-address <ipaddr>|igmp [snooping]|local-proxy-arp|nat inside|routing}
  ipv6 mld [snooping]
  no ...
  operstate up
  shutdown
```

Description

This command configures a VLAN interface.

Syntax

Parameter	Description	Range	Default
vlan	VLAN ID number.	1-4094	—
bandwidth-contract	Name of the bandwidth contract to be applied to this VLAN interface. When applied to a VLAN, the contract only limits multicast traffic and does not affect other data. Use the aaa bandwidth-contract command to configure a bandwidth contract.	—	—
description	String that describes this interface.	—	802.1Q VLAN
ip	Configures IPv4 for this interface.		
address	Configures the IP address for this interface, which can be one of the following: ■ <ipaddr> <netmask> ■ dhcp-client: use DHCP to obtain the IP address ■ pppoe: use PPPoE to obtain the IP address	—	—
helper-address	IP address of the DHCP server for relaying DHCP requests for this interface. If the DHCP server is on the same subnetwork as this VLAN interface, you do not need to configure this parameter.	—	—
igmp	Enables IGMP and/or IGMP snooping on this interface.	—	—
local-proxy-arp	Enables local proxy ARP.	—	—
nat inside	Enables source network address translation (NAT) for all traffic routed from this VLAN.	—	—
routing	Enables layer-3 forwarding on the VLAN interface. To disable layer-3 forwarding, you must configure the IP address for the interface and specify **no ip routing**.	—	(enabled)
ipv6	Configures IPv6 for this interface.		
mld	Enables Multicast Listener Discovery (MLD) on this interface.	—	—
snooping	Enables MLD snooping on this interface.	—	—
no	Negates any configured parameter.	—	—
operstate up	Set the state of the interface to be up.	—	—
shutdown	Causes a hard shutdown of the interface.	—	—

Usage Guidelines

All ports on the WLAN switch are assigned to VLAN 1 by default. Use the interface fastethernetlgigabitethernet command to assign a port to a configured VLAN.

Example

The following command configures a VLAN interface:

```
interface vlan 16
   ip address 10.26.1.1 255.255.255.0
   ip helper-address 10.4.1.22
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0. The **ipv6** parameters were introduced in AOS-W 3.3.

ip access-list eth

```
ip access-list eth {<number>|<name>}
  deny {<ethtype> [<bits>]|any} [mirror]
  no ...
  permit {<ethtype> [<bits>]|any} [mirror]
```

Description

This command configures an Ethertype access control list (ACL).

Syntax

Parameter	Description	Range	Default
`eth`	Enter a name, or a number in the specified range.	200-299	—
`deny`	Reject the specified packets, which can be one of the following: ■ Ethertype in decimal or hexadecimal (0-65535) and optional wildcard (0-65535) ■ any: match any Ethertype Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination.	—	—
`no`	Negates any configured parameter.	—	—
`permit`	Allow the specified packets, which can be one of the following: ■ Ethertype in decimal or hexadecimal (0-65535) and optional wildcard (0-65535) ■ any: match any Ethertype Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination.	—	—

Usage Guidelines

The Ethertype field in an Ethernet frame indicates the protocol being transported in the frame. This type of ACL filters on the Ethertype field in the Ethernet frame header, and is useful when filtering non-IP traffic on a physical port. This ACL can be used to permit IP frames while blocking other non-IP protocols such as IPX or Appletalk.

If you configure the mirror option, define the destination to which mirrored packets are sent in the firewall policy. For more information, see "firewall" on page 167.

Example

The following command configures an Ethertype ACL:

```
ip access-list eth 200
  deny 809b
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Policy Enforcement Firewall license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

The mirror parameter was introduced in AOS-W 3.3.

ip access-list extended

```
ip access-list extended {<number>|<name>}
  deny <protocol> <source> <dest>
  no ...
  permit <protocol> <source> <dest>
```

Description

This command configures an extended access control list (ACL).

Syntax

Parameter	Description	Range	Default
extended	Enter a name, or a number in the specified range.	100-199, 2000-2699	—
deny	Reject the specified packets.		
<protocol>	Protocol, which can be one of the following: ■ Protocol number between 0-255 ■ any: any protocol ■ icmp: Internet Control Message Protocol ■ igmp: Internet Gateway Message Protocol ■ tcp: Transmission Control Protocol ■ udp: User Datagram Protocol	—	—
<source>	Source, which can be one of the following: ■ Source address and wildcard ■ any: any source ■ host: specify a single host IP address	—	—
<dest>	Destination, which can be one of the following: ■ Destination address and wildcard ■ any: any destination ■ host: specify a single host IP address	—	—
no	Negates any configured parameter.	—	—
permit	Allow the specified packets.		
<protocol>	Protocol, which can be one of the following: ■ Protocol number between 0-255 ■ any: any protocol ■ icmp: Internet Control Message Protocol ■ igmp: Internet Gateway Message Protocol ■ tcp: Transmission Control Protocol ■ udp: User Datagram Protocol	—	—
<source>	Source, which can be one of the following: ■ Source address and wildcard ■ any: any source ■ host: specify a single host IP address	—	—

<dest>	Destination, which can be one of the following: ■ Destination address and wildcard ■ any: any destination ■ host: specify a single host IP address	—	—

Usage Guidelines

Extended ACLs are supported for compatibility with router software from other vendors. This ACL permits or denies traffic based on the source or destination IP address or IP protocol.

Example

The following command configures an extended ACL:

```
ip access-list extended 100
  deny any host 1.1.21.245 any
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Policy Enforcement Firewall license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip access-list mac

```
ip access-list mac {<number>|<name>}
  deny {<macaddr>[<wildcard>]|any|host <macaddr>} [mirror]
  no ...
  permit {<macaddr>[<wildcard>]|any|host <macaddr>} [mirror]
```

Description

This command configures a MAC access control list (ACL).

Syntax

Parameter	Description	Range	Default
`mac`	Configures a MAC access list. Enter a name, or a number in the specified range.	700-799, 1200-1299	—
`deny`	Reject the specified packets, which can be the following: ■ MAC address and optional wildcard ■ any: any packets ■ host: specify a MAC address Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination.	—	—
`no`	Negates any configured parameter.	—	—
`permit`	Allow the specified packets, which can be the following: ■ MAC address and optional wildcard ■ any: any packets ■ host: specify a MAC address Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination.	—	—

Usage Guidelines

MAC ACLs allow filtering of non-IP traffic. This ACL filters on a specific source MAC address or range of MAC addresses.

If you configure the mirror option, define the destination to which mirrored packets are sent in the firewall policy. For more information, see “firewall” on page 167.

Example

The following command configures a MAC ACL:

```
ip access-list mac 700
  deny 11:11:11:00:00:00
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Policy Enforcement Firewall license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

The mirror parameter was introduced in AOS-W 3.3.

ip access-list session

```
ip access-list session <name>
  <source> <dest> <service> <action> [<extended action>]
  no ...
```

Description

This command configures a session access control list (ACL).

Syntax

Parameter	Description	Range	Default
session	Enter a name for this ACL	—	—
<source>	The traffic source, which can be one of the following: ■ alias: specify the network resource (use the **netdestination** command to configure aliases; use the **show netdestination** command to see configured aliases) ■ any: match any traffic ■ host: specify a single host IP address ■ network: specify the IP address and netmask ■ user: represents the IP address of the user	—	—
<dest>	The traffic destination, which can be one of the following: ■ alias: specify the network resource (use the **netdestination** command to configure aliases; use the **show netdestination** command to see configured aliases) ■ any: match any traffic ■ host: specify a single host IP address ■ network: specify the IP address and netmask ■ user: represents the IP address of the user	—	—
<service>	Network service, which can be one of the following: ■ IP protocol number (0-255) ■ name of a network service (use the show netservice command to see configured services) ■ any: match any traffic ■ tcp: specify the TCP port number (0-65535) ■ udp: specify the UDP port number (0-65535)	—	—

<action>	Action if rule is applied, which can be one of the following: ■ deny: reject packets ■ dst-nat: perform destination NAT on packets ■ dual-nat: perform both source and destination NAT on packets ■ permit: forward packets ■ redirect: specify the location to which packets are redirected, which can be one of the following: ● datapath destination ID (0-65535) ● esi-group: specify the ESI server group configured with the esi group command ● opcode: specify the datapath destination ID (0x33, 0x34, or 0x82). Do not use this parameter without proper guidance from Alcatel-Lucent Networks. ● tunnel: specify the ID of the tunnel configured with the interface tunnel command ■ src-nat: perform source NAT on packets	—	—
<extended action>	Optional action if rule is applied, which can be one of the following: ■ blacklist: blacklist user ■ disable-scanning: pause ARM scanning while traffic is present ■ dot1p-priority: specify 802.1p priority (0-7) ■ log: generate a log message ■ mirror: mirror all session packets to datapath or remote destination If you configure the mirror option, define the destination to which mirrored packets are sent in the firewall policy. For more information, see "firewall" on page 167. ■ position: specify the position of the rule (1 is first, default is last) ■ queue: assign flow to priority queue (high/low) ■ send-deny-response: if <action> is deny, send an ICMP notification to the source ■ time-range: specify time range for this rule (configured with time-range command) ■ tos: specify ToS value (0-63)	—	—
no	Negates any configured parameter.	—	—

Usage Guidelines

Session ACLs define traffic and firewall policies on the WLAN switch. You can configure multiple rules for each policy, with rules evaluated from top (1 is first) to bottom. The first match terminates further evaluation. Generally, you should order more specific rules at the top of the list and place less specific rules at the bottom of the list. The ACL ends with an implicit deny all.

Example

The following command configures a session ACL that drops any traffic from 10.0.0.0 subnetwork:

```
ip access-list session drop-from10
   network 10.0.0.0 255.0.0.0 any any
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Policy Enforcement Firewall license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

ip access-list standard

```
ip access-list standard {<number>|<name>}
  deny {<ipaddr> <wildcard>|any|host <ipaddr>}
  no ...
  permit {<ipaddr> <wildcard>|any|host <ipaddr>}
```

Description

This command configures a standard access control list (ACL).

Syntax

Parameter	Description	Range	Default
`standard`	Enter a name, or a number in the specified range.	1-99, 1300-1399	—
`deny`	Reject the specified packets, which can be the following: ■ IP address and optional wildcard ■ any: any packets ■ host: specify a host IP address	—	—
`no`	Negates any configured parameter.	—	—
`permit`	Allow the specified packets, which can be the following: ■ IP address and optional wildcard ■ any: any packets ■ host: specify a host IP address	—	—

Usage Guidelines

Standard ACLs are supported for compatibility with router software from other vendors. This ACL permits or denies traffic based on the source address of the packet.

Example

The following command configures a standard ACL:

```
ip access-list standard 1
  permit host 10.1.1.244
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Policy Enforcement Firewall license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip cp-redirect-address

```
ip cp-redirect-address <ipaddr> | disable
```

Description

This command configures a redirect address for captive portal.

Syntax

Parameter	Description	Range	Default
`<ipaddr>`	Host address with a 32-bit netmask. This address should be routable from all external networks.	—	—
`disable`	Disables automatic DNS resolution for captive portal.	—	—

Usage Guidelines

This command redirects wireless clients that are on different VLANs (from the WLAN switch's IP address) to the captive portal on the WLAN switch.

If you have the Policy Enforcement Firewall license installed in the WLAN switch, modify the captiveportal session ACL to permit HTTP/S traffic to the destination cp-redirect instead of mswitch. If you do not have the Policy Enforcement Firewall license installed in the WLAN switch, the implicit captive-portal-profile ACL is automatically modified when you issue this command.

Example

The following command configures a captive portal redirect address:

```
ip cp-redirect-address
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip default-gateway

```
ip default-gateway <ipaddr> | import
```

Description

This command configures the default gateway for the WLAN switch.

Syntax

Parameter	Description	Range	Default
`<ipaddr>`	IP address of the default gateway.	—	—
`import`	Use the gateway IP address obtained through PPPoE or DHCP.	—	—

Usage Guidelines

Set the default gateway to the IP address of the interface on the upstream router or switch to which you connect the WLAN switch.

Example

The following command configures the default gateway for the WLAN switch:

```
ip default-gateway 10.1.1.1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip dhcp excluded-address

```
ip dhcp excluded-address <low-ipaddr> [<high-ipaddr>]
```

Description

This command configures an excluded address range for the DHCP server on the WLAN switch.

Syntax

Parameter	Description	Range	Default
`<low-ipaddr>`	Low end of range of IP addresses. For example, you can enter the IP address of the WLAN switch so that this address is not assigned.	—	—
`<high-ipaddr>`	High end of the range of IP addresses.	—	

Usage Guidelines

Use this command to specifically exclude certain addresses from being assigned by the DHCP server. It is good practice to exclude any statically assigned addresses.

Example

The following command configures an excluded address range:

```
ip dhcp excluded-address 192.168.1.1 192.168.1.255
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip dhcp pool

```
ip dhcp pool <name>
   default-router <ipaddr> ...
   dns-server {<ipaddr> ... |import}
   domain-name <name>
   lease <days> <hours> <minutes>
   netbios-name-server {<ipaddr> ... |import}
   network <ipaddr> {<netmask>|<prefix>}
   no ...
   option <code> ip <ipaddr>
```

Description

This command configures a DHCP pool on the WLAN switch.

Syntax

Parameter	Description	Range	Default
`default-router`	IP address of the default router for the DHCP client. The client should be on the same subnetwork as the default router. You can specify up to eight IP addresses.	—	—
`dns-server`	IP address of the DNS server, which can be one of the following:		
`<address>`	IP address of the DNS server. You can specify up to eight IP addresses.	—	—
`import`	Use the DNS server address obtained through PPPoE or DHCP.	—	—
`domain-name`	Domain name to which the client belongs.	—	—
`lease`	The amount of time that the assigned IP address is valid for the client. Specify the lease in <days> <hours> <minutes>.	—	—
`netbios-name-server`	IP address of the NetBIOS Windows Internet Naming Service (WINS) server, which can be one of the following:		
`<address>`	IP address of the WINS server. You can specify up to eight IP addresses.	—	—
`import`	Use the NetBIOS name server address obtained through PPPoE or DHCP.	—	—
`network`	Range of addresses that the DHCP server may assign to clients, in the form of <ipaddr> and <netmask> or <ipaddr> and <prefix> (/n).	—	—
`no`	Negates any configured parameter.	—	—
`option`	Client-specific option code and IP address. See RFC 2132, “DHCP Options and BOOTP Vendor Extensions”.	—	—

Usage Guidelines

A DHCP pool should be created for each IP subnetwork for which DHCP services should be provided. DHCP pools are not specifically tied to VLANs, as the DHCP server exists on every VLAN. When the WLAN switch receives a DHCP request from a client, it examines the origin of the request to determine if it should respond. If the IP address of the VLAN matches a configured DHCP pool, the WLAN switch answers the request.

Example

The following command configures a DHCP pool:

```
ip dhcp pool floor1
   default-router 10.26.1.1
   dns-server 192.168.1.10
   domain-name floor1.test.com
   lease 0 8 0
   network 10.26.1.0 255.255.255.0
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip domain lookup

```
ip domain lookup
```

Description

This command enables Domain Name System (DNS) hostname to address translation.

Syntax

There are no parameters for this command.

Usage Guidelines

This command is enabled by default. Use the no form of this command to disable.

Example

The following command enables DNS hostname translation:

```
ip domain lookup
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip domain-name

```
ip domain-name <name>
```

Description

This command configures the default domain name.

Syntax

Parameter	Description	Range	Default
`domain-name`	Name used to complete unqualified host names. Do not specify the leading dot (.).	—	—

Usage Guidelines

The WLAN switch uses the default domain name to complete hostnames that do not contain domain names. You must have at least one domain name server configured on the WLAN switch (see "ip name-server" on page 239).

Example

The following command configures the default domain name:

```
ip domain-name yourdomain.com
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip igmp

```
ip igmp
   last-member-query-count <number>
   last-member-query-interval <seconds>
   query-interval <seconds>
   query-response-interval <.1 seconds>
   robustness-variable <2-10>
   startup-query-count <number>
   startup-query-interval <seconds>
   version-1-router-present-timeout <seconds>
```

Description

This command configures Internet Group Management Protocol (IGMP) timers and counters.

Syntax

Parameter	Description	Range	Default
`last-member-query-count`	Number of group-specific queries that the WLAN switch sends before assuming that there are no local group members.	—	2
`last-member-query-interval`	Maximum time, in seconds, that can elapse between group-specific query messages.	—	10 seconds
`query-interval`	Interval, in seconds, at which the WLAN switch sends host-query messages to the multicast group address 224.0.0.1 to solicit group membership information.	1-1024	125 seconds
`query-response-interval`	Maximum time, in .1 seconds, that can elapse between when the WLAN switch sends a host-query message and when it receives a response. This must be less than the query-interval.	1-1024	100 (10 seconds)
`robustness-variable`	Increase this value to allow for expected packet loss on a subnetwork.	2-10	2
`startup-query-count`	Number of queries that the WLAN switch sends out on startup, separated by startup-query-interval. The default is the robustness-variable value.	—	2
`startup-query-interval`	Interval, in seconds, at which the WLAN switch sends general queries on startup. The default is 1/4 of the query-interval.	—	31 seconds
`version-1-router-present-timeout`	Timeout, in seconds, if a version 1 IGM router is detected.	—	400 seconds

Usage Guidelines

IGMP is used to establish and manage IP multicast group membership. See RFC 3376, “Internet Group Management Protocol, version 3” for more information.

Example

The following command configures IGMP:

```
ip igmp
   query-interval 130
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip local

```
ip local pool <name> <start-ipaddr> [<end-ipaddr>]
```

Description

This command configures a local IP pool for Layer-2 Tunnel Protocol (L2TP).

Syntax

Parameter	Description	Range	Default
`pool`	Name for the address pool.	—	—
`<start-ipaddr>`	Starting IP address for the pool.	—	—
`<end-ipaddr>`	(Optional) Ending IP address for the pool.	—	—

Usage Guidelines

VPN clients can be assigned IP addresses from the L2TP pool.

Example

The following command configures an L2TP pool:

```
ip local pool 10.1.1.1 10.1.1.99
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server and/or Remote AP license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip mobile active-domain

```
ip mobile active-domain <name>
```

Description

This command configures the mobility domain that is active on the WLAN switch.

Syntax

Parameter	Description	Range	Default
`active-domain`	Name of the mobility domain.	—	—

Usage Guidelines

All WLAN switches are initially part of the “default” mobility domain. If you use the “default” mobility domain, you do not need to specify this domain as the active domain on the WLAN switch. However, once you assign a WLAN switch to a user-defined domain, the “default” mobility domain is no longer an active domain on the WLAN switch.

Example

The following command assigns the WLAN switch to a user-defined mobility domain:

```
ip mobile active-domain campus1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 3.0.

ip mobile domain

```
ip mobile domain <name>
  hat <subnetwork> <mask> <vlan> <ha-ipaddr>
  no ...
```

Description

This command configures the mobility domain on the WLAN switch.

Syntax

Parameter	Description	Range	Default
domain	Name of the mobility domain.	—	—
hat	Configures a home agent table (HAT) entry.	—	—
<subnetwork>	Subnet that requires mobility service.	—	—
<mask>	Netmask for the IP address.	—	—
<vlan>	VLAN ID. The VLAN ID must be the VLAN number on the home agent WLAN switch.	1-4094	—
<ha-ipaddr>	IP address of the home agent.	—	—
no	Negates any configured parameter.	—	—

Usage Guidelines

You configure the HAT on a master WLAN switch; the mobility domain information is pushed to all local WLAN switches that are managed by the same master.

HAT entries map subnetworks or VLANs and the home agents. The home agent is typically the WLAN switch's IP address. The home agent's IP address must be routable; that is, all WLAN switches that belong to the same mobility domain must be able to reach the home agent's IP address.

The WLAN switch looks up information in the HAT to obtain the IP address of the home agent for a mobile client. Because there can be multiple home agents on a subnetwork, the HAT can contain more than one entry for the same subnetwork.

Example

The following command configures HAT entries:

```
ip mobile domain default
  hat 10.1.1.0 255.255.255.0 1 10.1.1.245
  hat 10.1.1.0 255.255.255.0 1 10.2.1.245
  hat 10.1.2.0 255.255.255.0 2 10.1.1.245
  hat 10.1.3.0 255.255.255.0 3 10.1.1.245
  hat 10.2.1.0 255.255.255.0 4 10.2.1.245
  hat 10.2.2.0 255.255.255.0 5 10.2.1.245
  hat 10.2.3.0 255.255.255.0 6 10.2.1.245
  hat 10.3.1.0 255.255.255.0 7 10.3.1.245
  hat 10.3.2.0 255.255.255.0 8 10.3.1.245
  hat 10.3.3.0 255.255.255.0 9 10.3.1.245
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

ip mobile foreign-agent

```
ip mobile foreign-agent {lifetime <seconds> | max-visitors <number> |
registrations {interval <msecs> | retransmits <number>}}
```

Description

This command configures the foreign agent for IP mobility.

Syntax

Parameter	Description	Range	Default
`lifetime`	Requested lifetime, in seconds, as per RFC 3344, “IP Mobility Support for IPv4”.	10-65534	180 seconds
`max-visitors`	Maximum number of active visitors.	0-5000	5000
`registrations`	Frequency at which re-registration messages are sent to the home agent:		
`interval`	Retransmission interval, in milliseconds	100-10000	1000 milliseconds
`retransmits`	Maximum number of times the foreign agent attempts mobile IP registration message exchanges before giving up.	0-5	3

Usage Guidelines

A foreign agent is the WLAN switch which handles all mobile IP communication with a home agent on behalf of a roaming client.

Example

The following command configures the foreign agent:

```
ip mobile foreign-agent registration interval 10000
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

ip mobile home-agent

```
ip mobile home-agent {max-bindings <number>|replay <seconds>}
```

Description

This command configures the home agent for IP mobility.

Syntax

Parameter	Description	Range	Default
`max-bindings`	Maximum number of mobile IP bindings. Note that there is a license-based limit on the number of users and a one user per binding limit in addition to unrelated users. This option is an additional limitation to control the maximum number of roaming users. When the limit is reached, registration requests from the foreign agent fail which causes a mobile client to set a new session on the visited WLAN switch, which will become its home WLAN switch.	0-5000	5000
`replay`	Time difference, in seconds, for timestamp-based replay protection, as described by RFC 3344, “IP Mobility Support for IPv4”. 0 disables replay.	0-300	7 seconds

Usage Guidelines

A home agent for a mobile client is the WLAN switch where the client first appears when it joins the mobility domain. The home agent is the single point of contact for the client when it roams.

Example

The following command configures the home agent:

```
ip mobile home-agent replay 100
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

ip mobile proxy

```
ip mobile proxy auth-sta-roam-only | block-dhcp-release | dhcp {max-requests <number>|
transaction-hold <seconds>|transaction-timeout <seconds>}|
event-threshold <number> | log-trail | no-service-timeout <seconds> | on-association |
re-home | stale-timeout <seconds> | stand-alone-AP | trail-length <number> |
trail-timeout <seconds> | tunnel-heartbeat {interval <seconds >|max-transmit <number>}
```

Description

This command configures the proxy mobile IP module in a mobility-enabled WLAN switch.

Syntax

Parameter	Description	Range	Default
`auth-sta-roam-only`	Allows a client to roam only if has been authenticated. If a client has not been authenticated, no mobility service is offered if it roams to a different VLAN or WLAN switch.	—	enabled
`block-dhcp-release`	Determines whether DHCP release packets generated from the client should be dropped or forwarded to the DHCP server. Blocking the packets prevents the DHCP server from assigning the same IP address to another client until the lease has expired.		disabled
`dhcp`	Configures proxy DHCP		
`max-requests`	Maximum number of BOOTP packets that are allowed to be handled during one DHCP session.	0-65534	25
`transaction-hold`	Hold time, in seconds, on proxy DHCP state after completion of DHCP transaction (DHCP ACK) was forwarded to the client. This option ensures that late BOOTP replies reach the station and that a retransmitted BOOTP request does not trigger a new proxy DHCP session.	1-600	5 seconds
`transaction-timeout`	Maximum time allowed for a proxy DHCP session to complete.	10-600	60 seconds
`event-threshold`	Maximum number of mobility events (events that can trigger mobility) handled per second. Mobility events above this threshold are ignored. This helps to control frequent mobility state changes when the client bounces back and forth on APs before settling down.	1-65535	25
`log-trail`	Enables logging at the notification level for mobile client moves.	—	enabled
`no-service-timeout`	Time, in seconds, after which mobility service expires. If nothing has changed from the previous state, the client is given another bridge entry but it will have limited connectivity.	30-60000	300 seconds
`on-association`	Mobility move detection is performed when the client associates with the WLAN switch instead of when the client sends packets. Enabled by default. Mobility on association can speed up roaming and improve connectivity for devices that do not send many uplink packets out that can trigger mobility. Downside is security; an association is all it takes to trigger mobility. This is irrelevant unless layer-2 security is enforced.	—	enabled
`re-home`	Allows on-hook phones to be assigned a new home agent. This is to load balance voice client home agents across WLAN switches in a mobility domain. **NOTE:** This parameter requires that you install the Voice Services Module license in the WLAN switch.	—	disabled

stale-timeout	Number of seconds the mobility state is retained after the loss of connectivity. This allows authentication state and mobility information to be preserved on the home agent WLAN switch. The default is 60 seconds but can be safely increased. Note that in many case a station state is deleted without waiting for the stale timeout; user delete from management, foreign agent to foreign agent handoff, etc. (This is different from the no-service-timeout; no-service-timeout occurs up front while the stale-timeout begins when mobility service is provided but the connection is disrupted for some reason.)	30-3600	60 seconds
stand-alone-AP	Enables support for third party or standalone APs. When this is enabled, broadcast packets are not used to trigger mobility and packets from untrusted interfaces are accepted.	—	disabled
trail-length	Specifies the maximum number of entries (client moves) stored in the user mobility trail.	1-100	30
trail-timeout	Specifies the maximum interval, in seconds, an inactive mobility trail is held.	120-86400	3600 seconds
tunnel-heartbeat	Configures settings for heartbeat exchange between the home agent and foreign agent:		
interval	Frequency, in seconds, at which heartbeat messages are exchanged.	1-10	2 seconds
max-transmit	Maximum number of heartbeat messages that can be lost before the IP-IP tunnel between the home agent and foreign agent is marked as “down”.	2-10	5

Usage Guidelines

The *proxy mobile IP module* in a mobility-enabled WLAN switch detects when a mobile client has moved to a foreign network and determines the home agent for a roaming client. The proxy mobile IP module performs the following functions:

- Derives the address of the home agent for a mobile client from the HAT using the mobile client’s IP address. If there is more than one possible home agent for a mobile client in the HAT, the proxy mobile IP module uses a discovery mechanism to find the current home agent for the client.
- Detects when a mobile client has moved. Client moves are detected based on ingress port and VLAN changes and mobility is triggered accordingly. For faster roaming convergence between AP(s) on the same WLAN switch, it is recommended that you keep the “on-association” option enabled. This helps trigger mobility as soon as 802.11 association packets are received from the mobile client.

Example

The following command enables re-home for voice clients:

```
ip mobile proxy re-home
```

NOTE: The re-home parameter requires the Voice Services Module.

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system. The re-home parameter requires the Voice Services Module.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

ip mobile revocation

```
ip mobile revocation {interval <msec>|retransmits <number>
```

Description

This command configures the frequency at which registration revocation messages are sent.

Syntax

Parameter	Description	Range	Default
`interval`	Retransmission interval, in milliseconds.	100-10000	1000 milliseconds
`retransmits`	Maximum number of times the home agent or foreign agent attempts mobile IP registration/revocation message exchanges before giving up.	0-5	3

Usage Guidelines

A home agent or foreign agent can send a registration revocation message, which revokes registration service for the mobile client. For example, when a mobile client roams from one foreign agent to another, the home agent can send a registration revocation message to the first foreign agent so that the foreign agent can free any resources held for the client.

Example

The following command configures registration revocation messages:

```
ip mobile revocation interval 2000
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

ip mobile trail

```
ip mobile trail {host IP address | host MAC address}
```

Description

This command configures the capture of association trail for all devices.

Syntax

Parameter	Description	Range	Default
`Host IP address`	The IP address of the client for which the association trail is captured.	—	disabled
`Host MAC address`	The MAC address of the client for which the association trail is captured.	—	disabled

Usage Guidelines

A device can move from one home agent to another or between home agents. When the client makes an association, the agent can store information about the client and registration time. The association trail can be captured for devices even when mobility is disabled.

Example

The following command configures trail capture for a client using its IP address:

```
ip mobile trail 1.2.3.4
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

ip name-server

```
ip name-server <ipaddr>
```

Description

This command configures servers for name and address resolution.

Syntax

Parameter	Description	Range	Default
`name-server`	IP address of the server.	—	—

Usage Guidelines

You can configure up to six servers using separate commands. Specify one or more servers when you configure a default domain name (see “ip domain-name” on page 225).

Example

The following command configures a name server:

```
ip name-server 10.1.1.245
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip nat

```
ip nat pool <name> <start-ipaddr> <end-ipaddr> [<dest-ipaddr>]
```

Description

This command configures a pool of IP addresses for network address translation (NAT).

Syntax

Parameter	Description	Range	Default
`pool`	Name of the NAT pool.	—	—
`<start-ipaddr>`	IP address that defines the beginning of the range of source NAT addresses in the pool.	—	—
`<end-ipaddr>`	IP address that defines the end of the range of source NAT addresses in the pool.	—	—
`<dest-ipaddr>`	Destination NAT IP address.	—	—

Usage Guidelines

This command configures a NAT pool which you can reference in a session ACL rule (see “ip access-list session” on page 214).

Example

The following command configures a NAT pool:

```
ip nat pool 2net 2.1.1.1 2.1.1.125
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Policy Enforcement Firewall license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip pppoe-max-segment-size

```
ip pppoe-max-segment-size <bytes>
```

Description

This command configures the maximum TCP segment size, in bytes, for Point-to-Point Protocol over Ethernet (PPPoE) data.

Syntax

Parameter	Description	Range	Default
`pppoe-max-segment-size`	Size, in bytes, of the maximum TCP segment.	128-1452	1452

Usage Guidelines

The maximum segment size for PPPoE is smaller than the normal Ethernet encapsulation size because of the PPPoE overhead.

Example

The following command configures the PPPoE maximum TCP segment size:

```
ip pppoe-max-segment-size 1412
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip pppoe-password

```
ip pppoe-password <string>
```

Description

This command configures the PPP over Ethernet (PPPoE) password.

Syntax

Parameter	Description	Range	Default
`pppoe-password`	PAP password configured on the PPPoE access concentrator.	—	—

Usage Guidelines

Note the following about enabling the PPPoE client on the WLAN switch:

- You cannot enable both the DHCP and PPPoE client on the WLAN switch at the same time.
- You can enable the PPPoE client on only one VLAN on the WLAN switch (the VLAN cannot be VLAN 1).
- You can connect only one port in the VLAN to the uplink switch.
- At least one interface in the VLAN must be in the up state before the PPPoE client requests an IP address from the server.

Example

The following commands configure the PPPoE client on the WLAN switch:

```
ip pppoe-service-name ppp2056
ip pppoe-username rudolph123
ip pppoe-password 1234567890
vlan 22
interface vlan 22
   ip address pppoe
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip pppoe-service-name

```
ip pppoe-service-name <string>
```

Description

This command configures the PPP over Ethernet (PPPoE) service name.

Syntax

Parameter	Description	Range	Default
`pppoe-service-name`	PPPoE service name.	—	—

Usage Guidelines

Note the following about enabling the PPPoE client on the WLAN switch:

- You cannot enable both the DHCP and PPPoE client on the WLAN switch at the same time.
- You can enable the PPPoE client on only one VLAN on the WLAN switch (the VLAN cannot be VLAN 1).
- You can connect only one port in the VLAN to the uplink switch.
- At least one interface in the VLAN must be in the up state before the PPPoE client requests an IP address from the server.

Example

The following commands configure the PPPoE client on the WLAN switch:

```
ip pppoe-service-name ppp2056
ip pppoe-username rudolph123
ip pppoe-password 1234567890
vlan 22
interface vlan 22
   ip address pppoe
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip pppoe-username

```
ip pppoe-username <string>
```

Description

This command configures the PPP over Ethernet (PPPoE) username.

Syntax

Parameter	Description	Range	Default
`pppoe-username`	PAP username configured on the PPPoE access concentrator.	—	—

Usage Guidelines

Note the following about enabling the PPPoE client on the WLAN switch:

- You cannot enable both the DHCP and PPPoE client on the WLAN switch at the same time.
- You can enable the PPPoE client on only one VLAN on the WLAN switch (the VLAN cannot be VLAN 1).
- You can connect only one port in the VLAN to the uplink switch.
- At least one interface in the VLAN must be in the up state before the PPPoE client requests an IP address from the server.

Example

The following commands configure the PPPoE client on the WLAN switch:

```
ip pppoe-service-name ppp2056
ip pppoe-username rudolph123
ip pppoe-password 1234567890
vlan 22
interface vlan 22
   ip address pppoe
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip radius

```
ip radius {nas-ip <ipaddr>|rfc-3576-server udp-port <port>|source-interface
{loopback|vlan <vlan>}
```

Description

This command configures global parameters for configured RADIUS servers.

Syntax

Parameter	Description	Range	Default
`nas-ip`	NAS IP address to send in RADIUS packets. A server-specific NAS IP configured with the **aaa authentication-server radius** command supersedes this configuration.	—	—
`rfc-3576-server`	Configures the UDP port to receive requests from a RADIUS server that can send user disconnect and change-of-authorization messages, as described in RFC 3576, "Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS)". See the **aaa rfc-3576-server** command to configure the server. **NOTE:** This parameter can only be used on the master WLAN switch.		
`udp-port`	UDP port to receive server requests.	0-65535	3799
`source-interface`	Interface for all outgoing RADIUS packets. The IP address of the specified interface is included in the IP header of RADIUS packets. The interface can be one of the following:		
`loopback`	The loopback interface.	—	—
`vlan`	The specified VLAN.	—	—

Usage Guidelines

This command configures global RADIUS server parameters. You configure specific RADIUS servers with the **aaa authentication-server radius** command.

Example

The following command configures a global NAS IP address sent in RADIUS packets:

```
ip radius nas-ip 192.168.1.245
```

NOTE: If the **aaa authentication-server radius** command configures a server-specific NAS IP, the server-specific IP address is used instead.

Platform Availability

This command is available on all platforms.

Licensing Requirements

The **ip radius rfc-3576-server udp-port** command requires the ESI license. Other commands are available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ip route

```
ip route <dest-ipaddr> <netmask> {<nexthop> [<cost>]|ipsec <map>}
```

Description

This command configures a static route on the WLAN switch.

Syntax

Parameter	Description	Range	Default
`route`	IP address and netmask of the destination network.	—	—
`<nexthop>`	IP address of the forwarding router.	—	—
`<cost>`	(Optional) Cost associated with this route. You can specify a cost to prioritize routes to the same destination. The lower the cost, the higher the priority.	—	—
`ipsec`	Name of the IPSec map for this route.	—	—

Usage Guidelines

This command configures a static route on the WLAN switch other than the default gateway. Use the **ip default-gateway** command to set the default gateway to the IP address of the interface on the upstream router or switch to which you connect the WLAN switch.

Example

The following command configures a static route:

```
ip route 172.16.0.0 255.255.0.0 10.1.1.200
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system. The **ipsec** parameter requires the VPN server license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

ipv6 access-list session

```
ipv6 access-list session <name>
  <source> <dest> <service> <action> [<extended action>]
  no ...
```

Description

This command configures a session access control list (ACL) for use with IPv6 clients.

Syntax

Parameter	Description
session	Enter a name for this ACL
<source>	The traffic source, which can be one of the following: ■ alias: specify the network resource **NOTE:** This release does not support IPv6 aliases. You cannot configure an alias for an IPv6 host or network. ■ any: match any traffic ■ host: specify a single host IPv6 address (for example, 2002:d81f:f9f0:1000:c7e:5d61:585c:3ab) ■ network: specify an IPv6 address and netmask (for example, 2002:ac10:fe:: ffff:ffff:ffff::) ■ user: represents the IPv6 address of the user
<dest>	The traffic destination, which can be one of the following: ■ alias: specify the network resource (use the show netdestination command to see configured aliases) **NOTE:** This release does not support IPv6 aliases. You cannot configure an alias for an IPv6 host or network. ■ any: match any traffic ■ host: specify a single host IPv6 address (for example, 2002:d81f:f9f0:1000:c7e:5d61:585c:3ab) ■ network: specify an IPv6 address and netmask (for example, 2002:ac10:fe:: ffff:ffff:ffff::) ■ user: represents the IPv6 address of the user
<service>	Network service, which can be one of the following: ■ IP protocol number (0-255) ■ name of a network service (use the show netservice command to see configured services) **NOTE:** Not all network services supported with IPv4 sessions ACLs are supported for IPv6. For example, you cannot use voice-related services (such as SIP or H323) for IPv6 session ACLs. ■ any: match any traffic ■ tcp: specify the TCP port number (0-65535) ■ udp: specify the UDP port number (0-65535)
<action>	Action if rule is applied, which can be one of the following: ■ deny: reject packets ■ permit: forward packets

<extended action>	Optional action if rule is applied, which can be one of the following: ■ blacklist: blacklist user ■ disable-scanning: pause ARM scanning while traffic is present ■ dot1p-priority: specify 802.1p priority (0-7) ■ log: generate a log message ■ mirror: mirror all session packets to datapath or remote destination ■ position: specify the position of the rule (1 is first, default is last) ■ queue: assign flow to priority queue (high/low) ■ send-deny-response: if <action> is deny, send an ICMP notification to the source ■ time-range: specify time range for this rule (configured with time-range command) ■ tos: specify ToS value (0-63)
no	Negates any configured parameter.

Usage Guidelines

Session ACLs define traffic and firewall policies on the WLAN switch. You can configure multiple rules for each policy, with rules evaluated from top (1 is first) to bottom. The first match terminates further evaluation. Generally, you should order more specific rules at the top of the list and place less specific rules at the bottom of the list. The ACL ends with an implicit deny all.

Example

The following command configures a session ACL that permits traffic from an IPv6 subnetwork:

```
ipv6 access-list session allow-ipv6-clients
  network 2002:ac10:fe:: ffff:ffff:ffff:: any any permit
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Policy Enforcement Firewall license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.3.

ipv6 firewall

```
ipv6 firewall {attack-rate {ping <number>|session <number>|tcp-syn <number>} |
deny-inter-user-bridging |
drop-ip-fragments |
enable-per-packet-logging |
enforce-tcp-handshake |
prohibit-ip-spoofing |
prohibit-rst-replay |
session-idle-timeout <seconds> |
session-mirror-destination <ipaddr>|<port>
```

Description

This command configures firewall options on the WLAN switch for IPv6 traffic.

Syntax

Parameter	Description	Range	Default
attack-rate	Sets rates which, if exceeded, can indicate a denial of service attack.		
ping	Number of ICMP pings per second, which if exceeded, can indicate a denial of service attack. Recommended value is 4	1-255	—
session	Number of TCP or UDP connection requests per second, which if exceeded, can indicate a denial of service attack. Recommended value is 32.	1-255	—
tcp-syn	Number of TCP SYN messages per second, which if exceeded, can indicate a denial of service attack. Recommended value is 32.	1-255	—
deny-inter-user-bridging	Prevents the forwarding of Layer-2 traffic between wired or wireless users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic. This option can be used to prevent Appletalk or IPX traffic from being forwarded.	—	disabled
drop-ip-fragments	When enabled, all IP fragments are dropped. You should not enable this option unless instructed to do so by an Alcatel-Lucent representative.	—	disabled
enable-per-packet-logging	Enables logging of every packet if logging is enabled for the corresponding session rule. Normally, one event is logged per session. If you enable this option, each packet in the session is logged. You should not enable this option unless instructed to do so by an Alcatel-Lucent representative, as doing so may create unnecessary overhead on the WLAN switch.	—	disabled
enforce-tcp-handshake	Prevents data from passing between two clients until the three-way TCP handshake has been performed. This option should be disabled when you have mobile clients on the network as enabling this option will cause mobility to fail. You can enable this option if there are no mobile clients on the network.	—	disabled
prohibit-ip-spoofing	Detects IP spoofing (where an intruder sends messages using the IP address of a trusted client). When this option is enabled, IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.	—	disabled

`prohibit-rst-replay`	Closes a TCP connection in both directions if a TCP RST is received from either direction. You should not enable this option unless instructed to do so by an Alcatel-Lucent representative.	—	disabled
`session-idle-timeout`	Time, in seconds, that a non-TCP session can be idle before it is removed from the session table. You should not modify this option unless instructed to do so by an Alcatel-Lucent representative.	16-259	15 seconds
`session-mirror-destination`	Destination to which mirrored session packets are sent. The destination can be either an IPv4 address or a WLAN switch port. You configure IPv6 flows to be mirrored with the **mirror** option of the **ipv6 access-list session** command. Use this option only for troubleshooting or debugging.	—	—

Usage Guidelines

This command configures global firewall options on the WLAN switch for IPv6 traffic.

Example

The following command disallows forwarding of non-IP frames between IPv6 clients:

```
ipv6 firewall deny-inter-user-bridging
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for noted parameters.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 3.3.

license

```
license {add <key>|del <key>|export <filename>|import <filename>|report <filename>}
```

Description

This command allows you to install, delete, and manage software licenses on the WLAN switch.

Syntax

Parameter	Description	Range	Default
`add`	Installs the software license key in the WLAN switch. The key is normally sent to you via email.	—	—
`del`	Removes the software license key from the WLAN switch. The key is normally sent to you via email.	—	—
`export`	Exports the license database on the WLAN switch to the specified file in flash.	—	—
`import`	Replaces the license database on the WLAN switch with the specified file in flash. The system serial numbers referenced in the imported file must match the numbers on the WLAN switch.	—	—
`report`	Saves a license report to the specified file in flash.	—	—

Usage Guidelines

Obtain an Alcatel-Lucent software license certificate from your Alcatel-Lucent sales representative or authorized reseller. Use the certificate ID and the system serial number to obtain a software license key which you install in the WLAN switch.

NOTE: For better usability, use the License Management page in the WebUI to install and manage licenses on the WLAN switch.

Example

The following command adds a license key on the WLAN switch:

```
license add 890BobXs-cVPCb3aJ-7FbCijhZ-BuQPtuI4-RjLJW6Pl-n5K
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode.

History

This command was available in AOS-W 3.0.

local-userdb add

```
local-userdb add {generate-username|username <name>} {generate-password|password
<passwd>} [email <email>] [expiry {duration <minutes>|time <hh/mm/yyy> <hh:mm>}] [mode
disable] [role <role>]
```

Description

This command creates a user account entry in the WLAN switch's internal database.

Syntax

Parameter	Description	Range	Default
`generate-username`	Automatically generate and add a username.	—	—
`username`	Add the specified username. The username can be up to 64 characters in length.	—	—
`generate-password`	Automatically generate a password for the username.	—	—
`password`	Add the specified password for the username. The password must be a minimum of 6 characters and can be up to 128 characters in length.	—	—
`email`	Email address for the use account.	—	—
`expiry`	Expiration for the user account. If this is not set, the account does not expire.	—	no expiration
`duration`	Duration, in minutes, for the user account.	1-2147483647	—
`time`	Date and time, in mm/dd/yyy and hh:mm format, that the user account expires.	—	—
`mode disable`	Disables the user account.	—	—
`role`	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.	—	guest

Usage Guidelines

When you specify the internal database as an authentication server, client information is checked against the user accounts in the internal database. You can modify an existing user account in the internal database with the **local-userdb modify** command, or delete an account with the **local-userdb del** command.

By default, the internal database in the master WLAN switch is used for authentication. Issue the **aaa authentication-server internal use-local-switch** command to use the internal database in a local WLAN switch; you then need to add user accounts to the internal database in the local WLAN switch.

Example

The following command adds a user account in the internal database with an automatically-generated username and password:

```
local-userdb add generate-username generate-password expiry duration 480
```

The following information is displayed when you enter the command:

```
GuestConnect
Username: guest4157
Password: cDFD1675
Expiration: 480 minutes
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system. The **role** parameter requires the PEF license.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

local-userdb del

```
local-userdb {del username <name>|del-all}
```

Description

This command deletes entries in the WLAN switch's internal database.

Syntax

Parameter	Description	Range	Default
`del username`	Deletes the user account for the specified username.	—	—
`del-all`	Deletes all entries in the internal database.	—	—

Usage Guidelines

User account entries created with expirations are automatically deleted from the internal database at the specified expiration. Use this command to delete an entry before its expiration or to delete an entry that was created without an expiration.

Example

The following command deletes a specific user account entry:

```
local-userdb del username guest4157
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

local-userdb export

```
local-userdb export <filename>
```

Description

This command exports the internal database to a file.

Syntax

Parameter	Description	Range	Default
`export`	Saves the internal database to the specified file in flash.	—	—

Usage Guidelines

After using this command, you can use the **copy** command to transfer the file from flash to another location.

Example

The following command saves the internal database to a file:

```
local-userdb export jan-userdb
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

local-userdb fix-database

```
local-userdb fix-database
```

Description

This command deletes and reinitializes the internal database.

Syntax

No parameters.

Usage Guidelines

Before using this command, you can save the internal database with the **local-userdb export** command.

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

local-userdb import

```
local-userdb import <filename>
```

Description

This command replaces the internal database with the specified file from flash.

Syntax

Parameter	Description	Range	Default
`import`	Replaces the internal database with the specified file.	—	—

Usage Guidelines

This command replaces the contents of the internal database with the contents in the specified file. The file must be a valid internal database file saved with the **local-userdb export** command.

Example

The following command imports the specified file into the internal database:

```
local-userdb import jan-userdb
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

local-userdb maximum-expiration

```
local-userdb maximum-expiration <minutes>
```

Description

This command configures the maximum time, in minutes, that a guest account in the internal database can remain valid.

Syntax

Parameter	Description	Range	Default
`maximum-expiration`	Maximum time, in minutes, that a guest account in the internal database can remain valid.	1-2147483647	—

Usage Guidelines

The user in the guest-provisioning role cannot create guest accounts that expire beyond the configured maximum time. This command is not available to the user in the guest-provisioning role.

Example

The following command sets the maximum time for guest accounts in the internal database to 8 hours (480 minutes):

```
local-userdb maximum-expiration 480
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.1.

local-userdb modify

```
local-userdb modify username <name> [email <email>] [expiry {duration <minutes>|time
<hh/mm/yyy> <hh:mm>}] [mode disable] [password <passwd>] [role <role>]
```

Description

This command modifies an existing user account entry in the WLAN switch's internal database.

Syntax

Parameter	Description	Range	Default
`username`	Name of the existing user account entry.	—	—
`email`	Email address for the user account.	—	—
`expiry`	Expiration for the user account. If this is not set, the account does not expire.	—	no expiration
`duration`	Duration, in minutes, for the user account.	—	—
`time`	Date and time, in mm/dd/yyy and hh:mm format, that the user account expires.	—	—
`mode disable`	Disables the user account.	—	—
`password`	New password for the username. The password must be a minimum of 6 characters and can be up to 128 characters in length.	—	—
`role`	Role for the user. **NOTE:** The Policy Enforcement Firewall license must be installed.	—	guest

Usage Guidelines

Use the **show local-userdb** command to view the current user account entries in the internal database.

Example

The following command disables an existing user account in the internal database:

```
local-userdb modify username guest4157 mode disable
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

localip

```
localip <ipaddr> ipsec <key>
```

Description

This command configures the IP address and preshared key for the local WLAN switch on a master WLAN switch.

Syntax

Parameter	Description	Range	Default
`<ipaddr>`	IP address of the local WLAN switch. Use the 0.0.0.0 address to configure a global preshared key for all inter-WLAN switch communications.	—	—
`ipsec`	Preshared key, which must be between 6-64 characters.	—	—

Usage Guidelines

Use this command on a master WLAN switch to configure the IP address and preshared key for communication with a local WLAN switch. On the local WLAN switch, use the **masterip** command to configure the IP address and preshared key for the master WLAN switch.

Example

The following command configures the local WLAN switch on a master WLAN switch:

```
localip 0.0.0.0 ipsec gw1234xyz
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

location

```
location <string>
```

Description

This command configures the location of the WLAN switch.

Syntax

Parameter	Description	Range	Default
`location`	A text string that specifies the system location.	—	—

Usage Guidelines

Use this command to indicate the location of the WLAN switch. You can use a combination of numbers, letters, characters, and spaces to create the name. To include a space in the name, use quotation marks to enclose the text string.

To change the existing name, enter the command with a different string. To unconfigure the location, enter “” at the prompt.

Example

The following command configures the location:

```
location “Building 10, second floor, room 21E”
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

logging

```
logging <ipaddr>
   [ap-debug <facility>] |
   [bssid-debug <facility>] |
   [essid-debug <facility>] |
   [network <facility>] |
   [security <facility>] |
   [system <facility>] |
   [user <facility>] |
   [user-debug <facility>] |
   [wireless <facility>] |
```

Description

Use this command to specify the IP address of the remote logging server, as well as facility log types and their associated facility levels.

Syntax

Parameter	Description	Range	Default
`ap-debug <facility>`	AP debug logs.	local0 to local7	local1
`bssid-debug <facility>`	Bssid debug logs.	local0 to local7	local1
`essid-debug <facility>`	Essid debug logs.	local0 to local7	local1
`network <facility>`	Network logs.	local0 to local7	local1
`security <facility>`	Security logs.	local0 to local7	local1
`system <facility>`	System logs.	local0 to local7	local1
`user <facility>`	User logs.	local0 to local7	local1
`user-debug <facility>`	User debug logs.	local0 to local7	local1
`wireless <facility>`	Wireless logs.	local0 to local7	local1

Usage Guidelines

The local use facilities (local0, local1, local2, local3, local4, local5, local6, and local7) are not reserved for specific message-generating sources, and can be used for sending syslog messages.

Use the `show logging` command to verify that the device sends logging messages.

Example

The following command adds the remote logging server with the IP address 10.1.2.3 with a user log type using local4.

```
logging 10.1.2.3 user local4
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 2.5.

logging console

```
logging console <level>
```

Description

Use this command to set the most inclusive level for which messages are logged.

Syntax

Parameter	Description	Range	Default
<level>	The message severity level, where <level> is one of the following: Emergencies, Alerts, Critical, Errors, Warnings, Notifications, Informational, or Debugging.	—	Informational (6)

Usage Guidelines

There are eight logging severity levels, each with its associated types of messages. Each level also includes every level below it. The higher the severity level, the more types of messages will be included in the log.

- Emergencies (0)—Panic conditions that occur when the system becomes unstable.
- Alerts (1)—Any condition requiring immediate attention and correction.
- Critical (2)—Any critical conditions, such as hard drive errors.
- Errors (3)—Error conditions.
- Warnings (4)—Warning messages.
- Notifications (5)—Significant events of a non-critical and normal nature.
- Informational (6)—Messages of general interest to system users.
- Debugging (7)—Messages containing information for debugging purposes.

Each level also includes every level below it. The higher the severity level, the more types of messages will be included in the log. Limit the types of messages logged by specifying a logging level. For example, if you set the logging level to informational, all messages from level 0 through level 5 (from emergencies through notifications) are logged.

If you do not specify a logging level value, the default is Informational.

Example

The following command sets the console logging level to Warnings.

```
logging console warnings
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 2.5.

The functionality of this command was deprecated in AOS-W 3.0. Although you can enter the command in the CLI, it has no effect.

logging facility

```
logging facility <facility>
```

Description

Use this command to set the facility to use when logging to the remote syslog server.

Syntax

Parameter	Description	Range	Default
`<facility>`	The facility to use when logging to a remote syslog server.	local0 to local7	—

Usage Guidelines

The local use facilities (local0, local1, local2, local3, local4, local5, local6, and local7) are not reserved for specific message-generating sources, and can be used for sending syslog messages.

Example

The following command sets the facility to `local4`.

```
logging facility local4
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 2.5.

logging level

```
logging level <level> <category> [process <process>] [subcat <subcategory>]
```

Description

Use this command to set the categories or subcategories and the severity levels of messages that are logged.

Syntax

Parameter	Description
<level>	The message severity level, which can be one of the following (in order of severity level):
emergencies	(0) Panic conditions that occur when the system becomes unstable.
alerts	(1) Any condition requiring immediate attention and correction.
critical	(2) Any critical conditions, such as hard drive errors.
errors	(3) Error conditions.
warnings	(4) Warning messages.
notifications	(5) Significant events of a non-critical and normal nature.
informational	(6) Messages of general interest to system users.
debugging	(7) Messages containing information for debugging purposes.
<category>	Message category, which can be one of the following:
ap-debug	AP troubleshooting messages. You must specify a debug value.
network	Network messages.
security	Security messages.
system	System messages.
user	User messages.
user-debug	User troubleshooting messages. You must specify a MAC address.
wireless	Wireless messages.
process	WLAN switch process, which can be one of the following:
aaa	AAA logging
ads	Anomaly detection
approc	AP processes
authmgr	User authentication
cfgm	Configuration Manager
crypto	VPN (IKE/IPSec)
cts	Transport service
dbsync	Database synchronization
dhcpd	DHCP packets
esi	External Services Interface
fpapps	Layer 2 and 3 control
httpd	Apache

`l2tp`	L2TP
`licensemgr`	License manager
`localdb`	Local database
`mobileip`	Mobile IP
`packetfilter`	Packet filtering of messaging and control frames
`phonehome`	PhoneHome
`pim`	Protocol Independent Multicast
`pppoed`	PPPoE
`pptp`	PPTP
`processes`	Run-time processes
`profmgr`	Profile Manager
`publisher`	Publish subscribe service
`rfm`	RF Troubleshooting Manager
`snmp`	SNMP
`stm`	Station management
`syslogdwrap`	Syslogd wrap
`traffic`	Traffic
`vrrpd`	VRRP
`wms`	Wireless management (master WLAN switch only)
`subcat`	Message subcategory, which depends upon the message category specified. The following lists the subcategories available for each message category: ■ ap-debug: all ■ network: all, dhcp, mobility, packet-dump ■ security: aaa, all, dot1x, firewall, ike, mobility, packet-trace, vpn, webserver ■ system: all, configuration, messages, snmp, webserver ■ user: all, captive-portal, dot1x, radius, vpn ■ user-debug: all, configuration ■ wireless: all

Usage Guidelines

There are eight logging severity levels, each with its associated types of messages. Each level also includes the levels below it. For example, if you set the logging level to informational (6), all messages from level 0 through level 5 (from emergencies through notifications) are also logged. The warnings severity level is set by default for all message categories and subcategories.

Example

The following command logs critical system messages.

```
logging level critical system
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 2.5.

logging monitor

```
logging monitor <level>
```

Description

Use this command to set the most inclusive terminal line (monitor) logging level.

Syntax

Parameter	Description	Range	Default
<level>	The message severity level, where <level> is one of the following: Emergencies, Alerts, Critical, Errors, Warnings, Notifications, Informational, or Debugging.	—	Informational (6)

Usage Guidelines

There are eight logging severity levels, each with its associated types of messages. Each level also includes every level below it. The higher the severity level, the more types of messages will be included in the log.

- Emergencies (0)—Panic conditions that occur when the system becomes unstable.
- Alerts (1)—Any condition requiring immediate attention and correction.
- Critical (2)—Any critical conditions, such as hard drive errors.
- Errors (3)—Error conditions.
- Warnings (4)—Warning messages.
- Notifications (5)—Significant events of a non-critical and normal nature.
- Informational (6)—Messages of general interest to system users.
- Debugging (7)—Messages containing information for debugging purposes.

Limit the types of messages logged by specifying a logging level. For example, if you set the logging level to informational, all messages from level 0 through level 5 (from emergencies through notifications) are logged.

If you do not specify a logging level value, the default is Informational.

Example

The following command sets the console logging level to Informational.

```
logging monitor informational
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 2.5.

The functionality of this command was deprecated in AOS-W 3.0. Although you can enter the command in the CLI, it has no effect.

loginsession

```
loginsession timeout <minutes>
```

Description

This command configures the time a management session (via Telnet or SSH) remains active without user activity.

Syntax

Parameter	Description	Range	Default
`timeout`	Number of minutes that a management session remains active without any user activity.	5-60, 0 to disable	15 minutes

Usage Guidelines

The management user must re-login to the WLAN switch after a Telnet or SSH session times out. If you set the timeout value to 0, sessions do not time out.

NOTE: The TCP session timeout for wireless and wired user sessions through the WLAN switch is 15 minutes; this timeout for user sessions is not configurable.

Example

The following command configures management sessions on the WLAN switch to not time out:

```
loginsession timeout 0
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

logout

```
logout
```

Description

This command exits the current CLI session.

Syntax

No parameters.

Usage Guidelines

Use this command to leave the current CLI session and return to the user login.

Example

The following command exits the CLI session:

```
(host) >logout
User:
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in user mode.

History

This command was available in AOS-W 3.0.

mac-address-table

```
mac-address-table static <macaddr> {fastethernet|gigabitethernet} <slot>/<port> vlan
<vlan>
```

Description

This command adds a static entry to the MAC address table.

Syntax

Parameter	Description	Range	Default
`<macaddr>`	Media Access Control (MAC) address, in the format xx:xx:xx:xx:xx:xx.	—	—
`<slot>`	<slot> is always 1 except for the OAW-6000 WLAN switch, where the slots can be 1, 2, or 3.	—	—
`<port>`	Number assigned to the network interface embedded in the WLAN switch or in the line card installed in the OAW-6000 WLAN switch. Port numbers start at 0 from the left-most position.		
`vlan`	ID number of the VLAN.	1-4094	—

Usage Guidelines

The MAC address table is used to forward traffic between ports on the WLAN switch. The table includes addresses learned by the WLAN switch. This command allows you to manually enter static addresses that are bound to specific ports and VLANs.

Example

The following command configures a MAC address table entry:

```
mac-address-table static 00:0b:86:f0:05:60 fastethernet 1/12 vlan 22
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

master-redundancy

```
master-redundancy
  master-vrrp <id>
  no ...
  peer-ip-address <ipaddr> ipsec <key>
```

Description

This command associates a VRRP instance with master WLAN switch redundancy.

Syntax

Parameter	Description	Range	Default
master-vrrp	The virtual router ID for the VRRP instance configured with the **vrrp** command.	1-255	
no	Negates any configured parameter.	—	—
peer-ip-address	IP address of the peer WLAN switch for master redundancy.	—	—
ipsec	Preshared key used to secure communications between the master WLAN switches. Specify a key of up to 64 bytes in length.	—	—

Usage Guidelines

To maintain a highly redundant network, you can use a WLAN switch as a standby for the master WLAN switch. The underlying protocol used is VRRP which you configure using the **vrrp** command.

Example

The following command configures VRRP for the initially preferred master WLAN switch:

```
vrrp 22
  vlan 22
  ip address 10.200.22.254
  priority 110
  preempt
  description Preferred-Master
  tracking master-up-time 30 add 20
  no shutdown
master-redundancy
  master-vrrp 22
  peer-ip-address 192.168.2.1 ipsec qwerTY012
```

The following shows the corresponding VRRP configuration for the peer WLAN switch.

```
vrrp 22
  vlan 22
  ip address 10.200.22.254
  priority 100
  preempt
  description Backup-Master
  tracking master-up-time 30 add 20
  no shutdown
master-redundancy
  master-vrrp 22
  peer-ip-address 192.168.22.1 ipsec qwerTY012
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

masterip

```
masterip <ipaddr> ipsec <key>
```

Description

This command configures the IP address and preshared key for the master WLAN switch on a local WLAN switch.

Syntax

Parameter	Description	Range	Default
`<ipaddr>`	IP address of the master WLAN switch.	—	—
`ipsec`	Preshared key, which must be between 6-64 characters.	—	—

Usage Guidelines

Use this command on a local WLAN switch to configure the IP address and preshared key for communication with the master WLAN switch. On the master WLAN switch, use the **localip** command to configure the IP address and preshared key for a local WLAN switch.

NOTE: Changing the IP address of the master on a local WLAN switch requires a reboot of the local WLAN switch.

Example

The following command configures the master WLAN switch on a local WLAN switch:

```
masterip 10.1.1.250 ipsec gw1234567
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

mgmt-user

```
mgmt-user <username> <role> <password>
mgmt-user localauth-disable
mgmt-user ssh-pubkey client-cert <certificate> <username> <role>
mgmt-user webui-cacert <name> serial <number> <username> <role>
```

Description

This command configures an administrative user.

Syntax

Parameter	Description	Range	Default
<username>	Name of the user. You can create a maximum of 10 management users. **NOTE:** If you configure a root management user, you can use special characters except for double-byte characters.	—	—
<role>	Role assigned to the user. Predefined roles include: ■ guest-provisioning: Allows the user to create guest accounts on a special WebUI page. ■ location-api-mgmt: Permits access to location API information. You can log into the CLI; however, you cannot use any CLI commands. ■ network-operations: Permits access to Monitoring, Reports, and Events pages in the WebUI. You can log into the CLI; however, you can only use a subset of CLI commands to monitor the WLAN switch. ■ read-only: Permits access to CLI show commands or WebUI monitoring pages only. ■ root: Permits access to all management functions on the WLAN switch.	—	—
<password>	**NOTE:** You are prompted for the <password> for this user after you type in <role> and press Enter. The password must have a minimum of six characters. You can use special characters in the management user password. Following are the restrictions: ■ You cannot use double-byte characters ■ You cannot use the question mark (?) ■ You cannot use white space <space >	—	—
localauth-disable	Disables authentication of management users based on the results returned by the authentication server. To cancel this setting, use the no form of the command: `no mgmt-user localauth-disable`. To verify if authentication of local management user accounts is enabled or disabled, use the following command: `show mgmt-user local-authentication-mode`	—	Enabled
ssh-pubkey	Configures certificate authentication of administrative users using the CLI through SSH.	—	—

client-cert	Name of the X.509 client certificate for authenticating administrative users using SSH.	—	—
<username>	Name of the user.	—	—
<role>	Role assigned to the authenticated user.	—	—
webui-cacert	Name of the client certificate for authenticating administrative users using the WebUI.	—	—
serial	Serial number of the client certificate.	—	—
<username>	Name of the user.	—	—
<role>	Role assigned to the authenticated user.	—	—

Usage Guidelines

You can configure client certificate authentication of WebUI or SSH management users (by default, only username/password is used). To configure certificate authentication for the WebUI or SSH, use the web-server mgmt-auth certificate or ssh mgmt-auth public-key commands, respectively.

Example

See the web-server and ssh command descriptions for examples of certificate and public key authentication. The following command configures a management user and role:

```
mgmt-user kgreen root
Password: *****
Re-Type password: *****
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0. The ssh-pubkey and webui-cacert parameters were introduced in AOS-W 3.1.

The network-operations role was introduced in AOS-W 3.2.

The location-api-mgmt role and localauth-disable parameters were introduced in AOS-W 3.3.

mobility-manager

```
mobility-manager <ipaddr> user <username> <password> [interval <secs>]
[retrycount <number>] [udp-port <port>] [rtls <rtls-udp-port>]
```

Description

This command allows the WLAN switch to communicate with an OV-MM server.

Syntax

Parameter	Description	Range	Default
`<ipaddr>`	IP address of the OV-MM server.	—	—
`user`	Name and SNMP password for the OV-MM server user.	—	—
`interval`	Round-trip time, in seconds, to trap server.	1-65535	60 seconds
`retrycount`	Number of retries to the OV-MM server before giving up.	1-65535	3
`udp-port`	UDP port number for trap server.	0-65535	162
`rtls`	UDP port number on which RSSI location data should be received from APs.	0-65535	8000

Usage Guidelines

This command needs to be configured before the WLAN switch can communicate with the OV-MM server. This command performs three tasks:

- Configures the IP address of the OV-MM server. In previous AOS-W releases, this was done with the mobility-server command.
- Creates an SNMP version 3 user profile with the configured <username> and <password>. This allows SNMP SETs from the OV-MM server to be received by the WLAN switch. The authentication protocol is Secure Hash Algorithm (SHA) and Data Encryption Standard (DES) is used for encryption. If <username> and <password> match an existing SNMP v3 user profile, the existing one is used. Otherwise, a new profile is created.

  This username and password must be used when adding this WLAN switch to the OV-MM server in the OV-MM Dashboard.
- Allows SNMP traps and notifications to be sent to the OV-MM server IP address, by adding this OV-MM server as a trap receiver.
- Optionally enables the OV-MM server to function as a Real Time Location System (RTLS) server to receive location information via APs from RTLS tags or other devices.

Use the **show mobility-manager** command to check the current status of the configured OV-MM servers.

Example

The following command configures the IP address and SNMP user profile for the OV-MM server:

```
mobility-manager 10.2.1.245 user mms-user my-password
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.1.

mux-address

```
mux-address <ipaddr>
```

Description

This command configures the IP address of a multiplexer (MUX) server.

Syntax

Parameter	Description	Range	Default
`mux-address`	IP address of the MUX server. This is the loopback or IP address of the WLAN switch acting as a MUX server.	—	—

Usage Guidelines

An OmniAccess WLAN switch can operate as a Wi-Fi MUX server, terminating GRE tunnels from MUX switches. As a Wi-Fi MUX server, the WLAN switch does not perform full Wi-Fi switching functions. Instead, it accepts traffic from ports designated as MUX ports, packages this traffic inside a GRE tunnel, and forwards the traffic back to a central WLAN switch for processing.

Example

The following command configures the address of a MUX server:

```
mux-address 192.168.1.245
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

netdestination

```
netdestination <name>
   host <ipaddr> [position <number>] |
   invert |
   network <ipaddr> <netmask> [position <number>] |
   no ... |
   range <start-ipaddr> <end-ipaddr> [position <number>]
```

Description

This command configures an alias for a network host, subnetwork, or range of addresses.

Syntax

Parameter	Description	Range	Default
`netdestination`	Name for this alias.	—	—
`host`	A single IP address.	—	—
`invert`	Specifies that the inverse of the network addresses configured are used. For example, if a network of 172.16.0.0 255.255.0.0 is configured, this parameter specifies that the alias matches everything except this subnetwork.	—	—
`network`	An IP subnetwork consisting of an IP address and netmask.	—	—
`no`	Negates any configured parameter.	—	—
`position`	Specifies the position of this network specification relative to other specifications (1 is first, default is last).	—	(last)
`range`	A range of IP addresses consisting of sequential addresses between a lower and an upper value. The maximum number of addresses in the range is 16. If larger ranges are needed, convert the range into a subnetwork and use the **network** parameter.	—	—

Usage Guidelines

Aliases can simplify configuration of session ACLs, as you can use an alias when specifying the traffic source and/or destination. Once you configure an alias, you can use it in multiple session ACLs.

Example

The following command configures an alias for an internal network:

```
netdestination Internal
   network 10.1.0.0 255.255.0.0
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Policy Enforcement Firewall license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

netservice

```
netservice <name> {<protocol> | tcp <port> [<port>] | udp <port> [<port>]}
[ALG <service>]
```

Description

This command configures an alias for network protocols.

Syntax

Parameter	Description	Range	Default
`netservice`	Name for this alias.	—	—
`<protocol>`	IP protocol number.	0-255	—
`tcp`	TCP port number. You can specify a single port number, or a port range (by specifying the lower and upper port number).	0-65535	—
`udp`	UDP port number. You can specify a single port number, or a port range (by specifying the lower and upper port number).	—	—
`ALG`	Application-level gateway (ALG) for this alias. Specify the applicable service (use the **?** to display available services).	—	—

Usage Guidelines

Aliases can simplify configuration of session ACLs, as you can use an alias when specifying the network service. Once you configure an alias, you can use it in multiple session ACLs.

Example

The following command configures an alias for a network service:

```
netservice HTTP tcp 80
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

ntp

```
ntp server <ipaddr> [iburst]
```

Description

This command configures a Network Time Protocol (NTP) server.

Syntax

Parameter	Description	Range	Default
`server`	IP address of the NTP server.	—	—
`iburst`	(Optional) This parameter causes the WLAN switch to send up to ten queries within the first minute to the NTP server. This option is considered “aggressive” by some public NTP servers.	—	disabled

Usage Guidelines

You can configure the WLAN switch to set its system clock using NTP by specifying one or more NTP servers.

Example

The following command configures an NTP server:

```
ntp server 10.1.1.245
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 1.0. The iburst option was introduced in 3.0.

packet-capture

```
packet-capture [other {disable | enable}] [sysmsg {all | disable | <opcodes>]
[tcp {all | disable | <ports>}] [udp {all | disable | <ports>]
```

Description

Use this command to enable or disable packet capturing and set packet capturing options on the control path for debugging purposes.

Syntax

Parameter	Description	Range	Default
`other`	Enable or disable all other types of packets. Specify up to ten comma-separated opcodes to capture; use `all` to sniff all opcodes; use `disable` to bypass the all setting. All CLI ports are always skipped.	—	Enabled
`sysmsg`	Enable or disable internal messaging packets.	—	Disabled
`tcp ports`	Enable or disable TCP packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all TCP ports; use `disable` to bypass the `all` setting. All CLI ports are always skipped.	—	Disabled
`udp ports`	Enable or disable UDP packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all UDP ports; use `disable` to bypass the `all` setting. All CLI ports are always skipped.	—	Disabled

Usage Guidelines

This command applies to control path; not for datapath packets. Packets can be retrieved through the `tar logs` command; look for the filter.pcap file. This command activates packet capture options on the current switch. They are not saved and applied across switches.

Example

The following command enables packet capturing for debugging a wireless WEP station doing VPN. This example uses the following parameters and values:

- Station up/down: sysmsg opcode 30
- WEP key plumbing: sysmsg opcode 29
- DHCP: sysmsg opcode 90
- IKE: UDP port 500 and 4500
- Layer 2 Tunneling Protocol (L2TP): UDP port 1701

```
packet-capture sysmsg 30,29,90 udp 500,4500,1701,1812,1645
```

Use the `show packet-capture` command to show the current action and the default.

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in privileged mode.

History

This command was available in AOS-W 2.3.

packet-capture-defaults

```
packet-capture-defaults [other {disable | enable}] [sysmsg {all | disable | <opcodes>]
[tcp {all | disable | <ports>}] [udp {all | disable | <ports>]
```

Description

Use this command to enable or disable packet capturing and set packet capturing options on the control path for debugging purposes.

Syntax

Parameter	Description	Range	Default
`other`	Enable or disable all other types of packets. Specify up to ten comma-separated opcodes to capture; use `all` to sniff all opcodes; use `disable` to bypass the all setting. All CLI ports are always skipped.	—	Enabled
`sysmsg`	Enable or disable internal messaging packets.	—	Disabled
`tcp ports`	Enable or disable TCP packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all TCP ports; use `disable` to bypass the `all` setting. All CLI ports are always skipped.	—	Disabled
`udp ports`	Enable or disable UDP packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all UDP ports; use `disable` to bypass the `all` setting. All CLI ports are always skipped.	—	Disabled

Usage Guidelines

This command applies to control path; not for datapath packets. Packets can be retrieved through the `tar logs` command; look for the filter.pcap file. This command sets defaults that go into the running-config file and can be saved and applied across switches.

Example

The following command enables packet capturing for debugging a wireless WEP station doing VPN. This example uses the following parameters and values:

- Station up/down: sysmsg opcode 30
- WEP key plumbing: sysmsg opcode 29
- DHCP: sysmsg opcode 90
- IKE: UDP port 500 and 4500
- Layer 2 Tunneling Protocol (L2TP): UDP port 1701

```
packet-capture-defaults sysmsg 30,29,90 udp 500,4500,1701,1812,1645
```

Use the `show-packet-capture-defaults` command to show the current action and the default.

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 2.3.

page

```
page <length>
```

Description

This command sets the number of lines of text the terminal will display when paging is enabled.

Syntax

Parameter	Description	Range	Default
`length`	Specifies the number of lines of text displayed.	24 - 100	—

Usage Guidelines

Use the `page` command in conjunction with the `paging` command to specify the number of lines of text to display. For more information on the pause mechanism that stops the command output from printing continuously to the terminal, see "paging" on page 294.

If you need to adjust the screen size, use your terminal application to do so.

Example

The following command sets 80 as the number of lines of text displayed:

```
page 80
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable and config modes on master WLAN switches.

History

This command was available in AOS-W 1.0.

paging

`paging`

Description

This command stops the command output from printing continuously to the terminal.

Syntax

No parameters.

Usage Guidelines

By default, paging is enabled.

With paging enabled, there is a pause mechanism that stops the command output from printing continuously to the terminal. If paging is disabled, the output prints continuously to the terminal. To disable paging, use the `no paging` command. You must be in enable mode to disable paging.

The paging setting is active on a per-user session. For example, if you disable paging from the CLI, it only affects that session. For new or existing sessions, paging is enabled by default.

You can also configure the number of lines of text displayed when paging is enabled. For more information, see the `page` command on page 293.

If you need to adjust the screen size, use your terminal application to do so.

Example

The following command enables paging:

```
paging
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable and config modes.

History

This command was available in AOS-W 1.0.

panic

```
panic {clear | info {file <filename> <symbolfile>|nvram <symbolfile>} | list {file
<filename>|nvram} | save <filename>}
```

Description

This command manages information created during a system crash.

Syntax

Parameter	Description
`clear`	Removes panic information from non-volatile random access memory (NVRAM).
`info`	Displays the content of specified panic files.
`list`	Lists panic information in the specified file in flash or in NVRAM.
`save`	Saves panic information from NVRAM into the specified file in flash.

Usage Guidelines

To troubleshoot system crashes, use the **panic save** command to save information from NVRAM into the specified file, then use the **panic clear** command to clear the information from NVRAM.

Example

The following command lists panic information in NVRAM:

```
panic list nvram
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

pcap

```
pcap raw-start <ipaddr> <target-ipaddr> <target-port> <format> [bssid <bssid>]
 [channel <number>]
pcap start <ipaddr> <filter> [bssid <bssid>] [channel <number>] [max-packet-size
 <size>] [max-packets <number>]
pcap interactive <ipaddr> <filter> <target-ipaddr> <target-port> [bssid <bssid>]
 [channel <number>]

pcap clear <ipaddr> <id> [bssid <bssid>]
pcap pause <ipaddr> <id> [bssid <bssid>]
pcap resume <ipaddr> <id> [bssid <bssid>]
pcap stop <ipaddr> <id> [bssid <bssid>]}
```

Description

These commands manage packet capture (PCAP) on OmniAccess air monitors.

Syntax

Parameter	Description	Range	Default
`<ipaddr>`	IP address of the air monitor collecting packets.	—	—
`<target-ipaddr>`	IP address of the client station running Wildpacket's AiroPeek monitoring application.	—	—
`<target-port>`	UDP port number on the client station where the captured packets are sent.	—	—
`<filter>`	Filter specification.	—	—
`<format>`	Format for captured packets, which is one of the following: 0 for pcap, 1 for peek, 2 for airmagnet.	—	—
`<id>`	ID of the PCAP session.	—	—
`bssid`	(Optional) BSSID of the interface for the PCAP session.	—	—
`channel`	(Optional) Number of a radio channel.	—	—
`max-packet-size`	(Optional) Maximum size of each captured packet. The maximum size is 128.	—	—
`max-packets`	(Optional) Maximum number of packets to be captured.	—	—

Usage Guidelines

These commands direct an OmniAccess air monitor to send packet captures to the Wildpacket's AiroPeek monitoring application on a remote client. The AiroPeek application listens for packets sent by the air monitor.

The following pcap commands are available:

`clear`	Clears the packet capture session.
`interactive`	Start an interactive packet capture session.
`pause`	Pause a packet capture session.
`raw-start`	Stream raw packets to an external viewer.
`resume`	Resume a packet capture session.
`start`	Start a new packet capture session.
`stop`	Stop a packet capture session.

Before using these commands, you need to start the AiroPeek application on the client and open a capture window for the air monitor. The AiroPeek application cannot be used to control the flow or type of packets sent from OmniAccess air monitors.

The AiroPeek application processes all packets, however, you can apply display filters on the capture window to control the number and type of packets being displayed. In the capture window, the time stamp displayed corresponds to the time that the packet is received by the client and is not synchronized with the time on the OmniAccess air monitor.

Example

The following command starts a raw packet capture session for the air monitor at 10.100.100.1 and sends the packets to the client at 192.168.22.44 on port 604 with pcap format:

```
pcap raw-start 10.100.100.1 192.168.22.44 604 0
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

ping

```
ping <ipaddress>
```

Description

This command sends five ICMP echo packets.

Syntax

Parameter	Description	Range	Default
`ipaddress`	Destination IP address.	—	—

Usage Guidelines

You can send five ICMP echo packets to a specified IP address. The WLAN switch times out after two seconds.

Example

The following example pings 10.10.10.5.

```
ping 10.10.10.5
```

The sample WLAN switch output is

```
Press 'q' to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.5, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.408/0.5434/1.073 ms
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in user, enable, and config modes.

History

This command was introduced in AOS-W 1.0.

pptp

```
pptp ip local pool <pool> <ipaddr> [<end-ipaddr>]
```

Description

This command configures an IP address pool for VPN users using Point-to-Point Tunneling Protocol (PPTP).

Syntax

Parameter	Description	Range	Default
`pool`	User-defined name for the address pool.	—	—
`<ipaddr>`	Starting IP address for the pool.	—	—
`<end-ipaddr>`	Ending IP address for the pool.	—	—

Usage Guidelines

If VPN is used as an access method, you specify the pool from which the user's IP address is assigned when the user negotiates a PPTP session. Use the **show vpdn pptp local** command to see the used and free addresses in the pool.

PPTP is an alternative to IPSec that is supported by various hardware platforms. PPTP is considered to be less secure than IPSec but also requires less configuration. You configure PPTP with the **vpdn** command.

Example

The following command configures an IP address pool for PPTP VPN users:

```
pptp ip local pool pptp-pool1 172.16.18.1 172.16.18.24
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN server license.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

priority-map

```
priority-map <name>
  dot1p <priority> high
  dscp <priority> high
  no ...
```

Description

This command configures the Type of Service (ToS) and Class of Service (CoS) values used to map traffic into high priority queues.

Syntax

Parameter	Description	Range	Default
<name>	User-defined name of the priority map.	—	—
dot1p	IEEE 802.1p priority value or range of values (separated by -).	0-7	—
dscp	Differentiated Services Code Point (DSCP) priority value or range of values (separated by -).	0-63	—
no	Negates any configured parameter.	—	—

Usage Guidelines

This command allows you inbound traffic that is already tagged with 802.1p and/or IP ToS into hardware queues. You apply configured priority maps to ports on the WLAN switch (using the **interface fastethernet** or **interface gigbitethernet** command). This causes the WLAN switch to inspect inbound traffic on the port; when a matching QoS tag is found, the packet or flow is mapped to the specified queue.

Example

The following commands configure a priority map and apply it to a port:

```
priority-map pri1
  dscp 4-20 high
  dscp 60 high
  dot1p 4-7 high
interface gigabitethernet 1/24
  priority-map pri1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

process

```
process restart <name> [core]
```

Description

This command restarts a process on the WLAN switch.

Syntax

Parameter	Description	Default
`restart`	Name of the process to be restarted.	—
`core`	Creates a core file.	—

Usage Guidelines

You should not typically need to run this command. However, if a **show** command fails to return, a "Module <name> not responding" message appears, or logs indicate that there is a communication failure, you can restart a process. You can restart any process shown with the **show processes** command.

Example

The following command restarts the WMS module and generates a core file for analysis.

```
process restart wms core
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode.

History

This command was available in AOS-W 3.0.

prompt

```
prompt <prompt>
```

Description

This command changes the prompt text.

Syntax

Parameter	Description	Range	Default
`prompt`	The prompt text displayed by the WLAN switch.	1–64	<hostname>

Usage Guidelines

You can use any alphanumeric character, punctuation, or symbol character. To use spaces, plus symbols (+), question marks (?), or asterisks (*), enclose the text in quotes.

You cannot alter the parentheses that surround the prompt text, or the greater-than (>) or hash (#) symbols that indicate user or enable CLI mode.

Example

The following example changes the prompt text to “It’s a new day!”.

```
(host) (config) #prompt “It’s a new day!”
(It’s a new day!) (config) #
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 1.0.

provision-ap

```
provision-ap
   a-ant-bearing <bearing>
   a-ant-gain <gain>
   a-ant-tilt-angle <angle>
   a-antenna {1|2|both}
   altitude <altitude>
   ap-group <group>
   ap-name <name>
   copy-provisioning-params {ap-name <name> | ip-addr <ipaddr>}
   dns-server-ip <ipaddr>
   domain-name <name>
   external-antenna
   fqln <name>
   g-ant-bearing <bearing>
   g-ant-gain <gain>
   g-ant-tilt-angle <angle>
   g-antenna {1|2|both}
   gateway <ipaddr>
   ikepsk <key>
   ipaddr <ipaddr>
   latitude <location>
   longitude <location>
   master {<name>|<ipaddr>}
   mesh-role {mesh-point|mesh-portal|none}
   netmask <netmask>
   no ...
   pap-passwd <string>
   pap-user <name>
   pppoe-passwd <string>
   pppoe-service-name <name>
   pppoe-user <name>
   read-bootinfo {ap-name <name>|ip-addr <ipaddr>|wired-mac <macaddr>}
   reprovision {all|ap-name <name>|ip-addr <ipaddr>|serial-num <string>|
    wired-mac <macaddr>}
   reset-bootinfo {ap-name <name>|ip-addr <ipaddr>|wired-mac <macaddr>}
   server-ip <ipaddr>
   server-name <name>
   syslocation <string>
```

Description

This command provisions or reprovisions an AP.

Syntax

Parameter	Description	Range	Default
a-ant-bearing	Determines the horizontal coverage distance of the 802.11a (5GHz) antenna from True North. From a planning perspective, the horizontal coverage pattern does not consider the elevation or vertical antenna pattern. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	0-360 Decimal Degrees	—
a-ant-gain	Antenna gain for 802.11a (5GHz) antenna.	—	—

a-ant-tilt-angle	Directs the angle of the 802.11a (5GHz) antenna for optimum coverage. Use a - (negative) value for downtilt and a + (positive) value for uptilt. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	-90 to +90 Decimal Degrees	—
a-antenna	Antenna use for 5 GHz (802.11a) frequency band. ■ 1: Use antenna 1 ■ 2: Use antenna 2 ■ both: Use both antennas	1, 2, both	both
altitude	Altitude, in meters, of the AP. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	—	—
ap-group	Name of the AP group to which the AP belongs.	—	"default"
ap-name	Name for this AP.	—	—
copy-provisioning-params	Initializes the provisioning-params workspace with the current provisioning parameters of the specified AP, The provisioning parameters of the AP must have previously been retrieved with the **read-bootinfo** option. **NOTE:** This parameter can only be used on the master WLAN switch.	—	—
dns-server-ip	IP address of the DNS server for the AP.	—	—
domain-name	Domain name for the AP.	—	—
external-antenna	Use an external antenna with the AP.	—	—
fqln	Fully-qualified location name (FQLN) for the AP, in the format <APname.floor.building.campus>.	—	—
g-ant-bearing	Determines the horizontal coverage distance of the 802.11g (2.4GHz) antenna from True North. From a planning perspective, the horizontal coverage pattern does not consider the elevation or vertical antenna pattern. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	0-360 decimal degrees	—
g-ant-gain	Antenna gain for 802.11g (2.4GHz) antenna.	—	—
g-ant-tilt-angle	Directs the angle of the 802.11g (2.4GHz) antenna for optimum coverage. Use a - (negative) value for downtilt and a + (positive) value for uptilt. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	-90 to +90 Decimal Degrees	—
g-antenna	Antenna use for 2.4 GHz (802.11g) frequency band. ■ 1: Use antenna 1 ■ 2: Use antenna 2 ■ both: Use both antennas	1, 2, both	both
gateway	IP address of the default gateway for the AP.	—	—

`ikepsk`	IKE preshared key for the AP. **NOTE:** The Remote AP license must be installed.	—	—
`ipaddr`	Static IP address for the AP.	—	—
`latitude`	Latitude coordinates of the AP. Use the format: Degrees, Minutes, Seconds (DMS). For example: 37 22 00 N	—	—
`longitude`	Longitude coordinates of the AP. Use the DMS format. For example: 122 02 00 W	—	—
`master`	Name or IP address for the master WLAN switch.	—	—
`mesh-role`	Configure the AP to operate as a mesh node. You assign one of two roles: mesh portal or mesh point. If you select "none," the AP operates as a thin AP. **NOTE:** The Secure Enterprise Mesh license must be installed.	—	—
`netmask`	Netmask for the IP address.	—	—
`no`	Negates any configured parameter.	—	—
`pap-passwd`	Password Authentication Protocol (PAP) password for the AP. You can use special characters in the PAP password. Following are the restrictions: ■ You cannot use double-byte characters ■ You cannot use a tilde (~) ■ You cannot use a tick (') ■ If you use quotes (single or double), you must use the backslash (\) before and after the password **NOTE:** The Remote AP license must be installed.	—	—
`pap-user`	PAP username for the AP. **NOTE:** The Remote AP license must be installed.	—	—
`pppoe-passwd`	Point-to-Point Protocol over Ethernet (PPPoE) password for the AP. **NOTE:** The Remote AP license must be installed.	—	—
`pppoe-service-name`	PPPoE service name for the AP. **NOTE:** The Remote AP license must be installed.	—	—
`pppoe-user`	PPPoE username for the AP. **NOTE:** The Remote AP license must be installed.	—	—
`read-bootinfo`	Retrieves current provisioning parameters of the specified AP. **NOTE:** This parameter can only be used on the master WLAN switch.	—	—
`reprovision`	Provisions one or more APs with the values in the provisioning-params workspace. To use **reprovision**, you must use **read-bootinfo** to retrieve the current values of the APs into the provisioning-ap-list. **NOTE:** This parameter can only be used on the master WLAN switch.	—	—
`reset-bootinfo`	Restores factory default provisioning parameters to the specified AP. **NOTE:** This parameter can only be used on the master WLAN switch.	—	—

server-ip	IP address of the WLAN switch from which the AP boots.	—	—
server-name	DNS name of the WLAN switch from which the AP boots.	—	—
syslocation	User-defined description of the location of the AP.	—	—

Usage Guidelines

You do not need to provision APs before installing and using them.

The exceptions are:

- The OAW-AP60 and OAW-AP80, which have antenna gains that you must provision before they can be used.
- APs configured for mesh. You must provision the AP before you install it as a mesh node in a mesh deployment.

NOTE: For better usability, use the Provisioning page in the WebUI to provision an AP.

Provisioned or reprovisioned values do not take effect until the AP is rebooted. APs reboot automatically after they are successfully reprovisioned.

Provisioning a Single AP

To provision a single AP:

1. Use the **read-bootinfo** option to read the current information from the deployed AP you wish to reprovision.
2. Use the **show provisioning-ap-list** command to see the AP to be provisioned.
3. Use the **copy-provisioning-params** option to copy the AP's parameter values to the provisioning-params workspace.
4. Use the provision-ap options to set new values. Use the **show provisioning-params** command to display parameters and values in the provisioning-params workspace. Use the **clear provisioning-params** command to reset the workspace to default values.
5. Use the **reprovision** option to provision the AP with the values in provisioning-params workspace. The AP automatically reboots.

Provisioning Multiple APs at a Time

You can change parameter values for multiple APs at a time, however, note the following:

- You cannot provision the following AP-specific options on multiple APs:
  - ap-name
  - ipaddr
  - pap-user
  - pap-passwd
  - ikepsk

  If any of these options are already provisioned on the AP, their values are retained when the AP is reprovisioned.
- The values of the server-name, a-ant-gain, or g-ant-gain options are retained if they are not reprovisioned.
- All other values in the provisioning-params workspace are copied to the APs.

To provision multiple APs at the same time:

1. Use the **read-bootinfo** to read the current information from each deployed AP that you wish to provision.

NOTE: The AP parameter values are written to the provisioning-ap-list. To reprovision multiple APs, the APs must be present in the provisioning-ap-list. Use the **show provisioning-ap-list** command to see the APs that will be provisioned. Use the **clear provisioning-ap-list** command to clear the provisioning-ap-list.

2. Use the **copy-provisioning-params** option to copy an AP's parameter values to the provisioning-params workspace.
3. Use the provision-ap options to set new values. Use the **show provisioning-params** command to display parameters and values in the provisioning-params workspace. Use the **clear provisioning-params** command to reset the workspace to default values.
4. Use the **reprovision all** option to provision the APs in the provisioning-ap-list with the values in provisioning-params workspace. All APs in the provisioning-ap-list automatically reboot.

The following are useful commands when provisioning one or more APs:

- **show|clear provisioning-ap-list** displays or clears the APs that will be provisioned.
- **show|clear provisioning-params** displays or resets values in the provisioning-params workspace.
- **show ap provisioning** shows the provisioning parameters an AP is currently using.

Example

The following commands change the IP address of the master WLAN switch on the AP:

```
provision-ap
  read-bootinfo ap-name lab103
  show provisioning-ap-list
  copy-provisioning-params ap-name lab103
  master 10.100.102.210
  reprovision ap-name lab103
```

Platform Availability

This command is available on all platforms, except for the noted parameters.

Licensing Requirements

This command is available in the base operating system, except for the noted parameters.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 3.0.

Support for the mesh parameters, additional antenna parameters, and AP location parameters was introduced in AOS-W 3.2.

rap-wml

```
rap-wml <server-name> [ageout <period>] [cache {disable|enable}] [db-name <name>]
[ip-addr <ipaddr>] [password <password>] [type {mssql|mysql}] [user <name>]
```

Description

Use this command to specify the name and attributes of a MySQL or an MSSQL server.

Syntax

Parameter	Description	Range	Default
ageout	(Optional.) Specifies the cache ageout period, in seconds.	—	0
cache	(Optional.) Enables the cache, or disables the cache.	—	Disabled
db-name	(Optional.) Specifies the name of the MySQL or MSSQL database.	—	—
ip-addr	(Optional.) Specifies the IP address of the named MSSQL server.	—	0.0.0.0
no	Negates any configured parameter.	—	—
password	(Optional.) Specifies the password required for database login.	—	—
type	(Optional.) Specifies the server type.	—	—
user	(Optional.) Specifies the user name required for database login.	—	—

Usage Guidelines

Use the `show rap-wml cache` command to show the cache of all lookups for a database server. Use the `show rap-wml servers` command to show the database server state. Use the `show rap-wml wired-mac` command to show wired MAC Discovered on traffic through the AP.

Example

This example configures a MySQL server and sets up associated rap-wml table attributes.

```
rap-wml mysqlserver type mysql ip-addr 10.4.11.10 db-name automatedtestdatabase
   user sa password sa
rap-wml table mysqlserver mactest_undelimited mac timestamp-column time 600
rap-wml table mysqlserver mactest_delimited mac delimiter : timestamp-column time 600
```

This example configures an MSSQL server and sets up associated rap-wml table attributes.

```
rap-wml mssqlserver type mssql ip-addr 10.4.11.11 db-name automatedtestdatabase
   user sa password sa
rap-wml table mssqlserver mactest_undelimited mac timestamp-column time 600
rap-wml table mssqlserver mactest_delimited mac delimiter : timestamp-column time 600
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Wireless Intrusion Protection license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 2.0.

rap-wml table

```
rap-wml table <server-name> <table-name> <column-name> {[delimiter <char>] |
[timestamp-column <timestamp-column-name> <lookup-time>]}
```

Description

Use this command to specify the name and attributes of the database table to be used for lookup.

Syntax

Parameter	Description	Range	Default
`server-name`	Specifies the database server name (created using the `rap-wml <server-name>` command.	—	—
`table-name`	Specifies the database table name.	—	—
`column-name`	Specifies the database column name with the MAC address.	—	—
`delimiter`	Specifies the optional delimiter character for the MAC address in the database.	—	No delimiter
`no`	Negates the rap-wml table for the named server.	—	—
`timestamp-column`	Specify the database column name with the timestamp last seen.	—	—
`timestamp-column-name`	Specify the database column name with the timestamp last seen.	—	—
`lookup-time`	Specifies how far back—in seconds—to look for the MAC address. Use 0 seconds to lookup everything.	—	0

Usage Guidelines

Use the `rap-wml <servername>` command to configure a MySQL or an MSSQL server, then use the `rap-wml table` command to configure the associated database table for the server.

Example

This example configures a MySQL server and sets up associated rap-wml table attributes for that server.

```
rap-wml mysqlserver type mysql ip-addr 10.4.11.10 db-name automatedtestdatabase
   user sa password sa
rap-wml table mysqlserver mactest_undelimited mac timestamp-column time 600
rap-wml table mysqlserver mactest_delimited mac delimiter : timestamp-column time 600
```

This example configures an MSSQL server and sets up associated rap-wml table attributes for that server.

```
rap-wml mssqlserver type mssql ip-addr 10.4.11.11 db-name automatedtestdatabase
   user sa password sa
rap-wml table mssqlserver mactest_undelimited mac timestamp-column time 600
rap-wml table mssqlserver mactest_delimited mac delimiter : timestamp-column time 600
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Wireless Intrusion Protection license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 2.0.

reload

```
reload
```

Description

This command performs a reboot of the WLAN switch.

Syntax

No parameters.

Usage Guidelines

Use this command to reboot the WLAN switch if required after making configuration changes or under the guidance of Alcatel-Lucent customer support. The `reload` command powers down the WLAN switch, making it unavailable for configuration. After the WLAN switch reboots, you can access it via a local console connected to the serial port, or through an SSH, Telnet, or WebUI session. If you need to troubleshoot the WLAN switch during a reboot, use a local console connection.

After you use the `reload` command, the WLAN switch prompts you for confirmation of this action. If you have not saved your configuration, the WLAN switch returns the following message:

```
Do you want to save the configuration(y/n):
```

- Enter `y` to save the configuration.
- Enter `n` to not save the configuration.
- Press [Enter] to exit the command without saving changes or rebooting the WLAN switch.

If your configuration has already been saved, the WLAN switch returns the following message:

```
Do you really want to reset the system(y/n):
```

- Enter `y` to reboot the WLAN switch.
- Enter `n` to cancel this action.

NOTE: The command will timeout if you do not enter `y` or `n`.

Example

The following command assumes you have already saved your configuration and you must reboot the WLAN switch:

```
reload
```

The WLAN switch returns the following messages:

```
Do you really want to reset the system(y/n): y
System will now restart!
...
Restarting system.
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable and config modes.

History

This command was available in AOS-W 1.0.

reload-peer-sc

`reload-peer-sc`

Description

This command performs a reboot of the OmniAccess Supervisor Card I or II (OAW-SC) in OmniAccess 6000 WLAN switches.

Syntax

No parameters.

Usage Guidelines

This command is supported only on WLAN switches that require the OmniAccess Supervisor Card I or II (OAW-SC). The OAW-SC processes all traffic from the line cards (LCs) and performs all management functions.

NOTE: This command is not applicable to the OmniAccess Supervisor Card III (OAW-S3).

The `reload-peer-sc` command allows one OAW-SC to reset the other OAW-SC in a dual OAW-SC configuration. This does not affect the OAW-SC on which the command is executed and the LCs which it controls.

After you use the `reload-peer-sc` command, the WLAN switch prompts you for confirmation of this action and returns the following message:

```
Do you really want to reset the peer Supervisor Card(y/n):
```

- Enter `y` to reboot the peer OAW-SC.
- Enter `n` to cancel this action.

NOTE: The command will timeout if you do not enter `y` or `n`.

Example

The following command reboots the peer OAW-SC:

```
reload-peer-sc
```

The WLAN switch returns the following messages:

```
Do you really want to reset the peer Supervisor Card(y/n):
Peer Supervisor Card will now restart.
```

Platform Availability

This command is only available on the OmniAccess 6000 WLAN switch.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable and config modes.

History

This command was available in AOS-W 1.0.

rename

```
rename <filename> <newfilename>
```

Description

This command renames an existing system file.

Syntax

Parameter	Description	Range	Default
`filename`	An alphanumeric string that specifies the current name of the file on the system.	—	—
`newfilename`	An alphanumeric string that specifies the new name of the file on the system.	—	—

Usage Guidelines

Use this command to rename an existing system file on the WLAN switch. You can use a combination of numbers, letters, and punctuation (periods, underscores, and dashes) to rename a file. The new name takes affect immediately.

Make sure the renamed file uses the same file extension as the original file. If you change the file extension, the file may be unrecognized by the system. For example, if you have an existing file named `upgrade.log`, the new file must include the `.log` file extension.

You cannot rename the active configuration currently selected to boot the WLAN switch. If you attempt to rename the active configuration file, the WLAN switch returns the following message:

```
Cannot rename active configuration file
```

To view a list of system files, and for more information about the directory contents, see “dir” on page 148.

Example

The following command changes the file named test_configuration to deployed_configuration:

```
rename test_configuration deployed_configuration
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable and config modes on master WLAN switches.

History

This command was available in AOS-W 1.0.

restore

```
restore flash
```

Description

This command restores flash directories backed up to the flashbackup.tar.gz file.

Syntax

Parameter	Description	Range	Default
`flash`	Restores flash directories from the flashbackup.tar.gz file.	—	—

Usage Guidelines

Use the **backup flash** command to tar and compress flash directories to the flashbackup.tar.gz file.

Example

The following command restores flash directories from the flashbackup.tar.gz file:

```
restore flash
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

rf arm-profile

```
rf arm-profile <profile>
  40MHz-allowed-bands {All|None|a-only|g-only}
  acceptable-coverage-index <number>
  active-scan (not intended for use)
  assignment {disable|maintain|multi-band|single-band}
  backoff-time <seconds>
  client-aware
  clone <profile>
  error-rate-threshold <percent>
  error-rate-wait-time <seconds>
  free-channel-index <number>
  ideal-coverage-index <number>
  load-aware-scan-threshold (not intended for use)
  max-tx-power <dBm>
  min-scan-time <seconds>
  min-tx-power <dBm>
  mode-aware (not intended for use)
  multi-band-scan
  no ...
  noise-threshold <number>
  noise-wait-time <seconds>
  ps-aware-scan
  rogue-ap-aware
  scan-interval <seconds>
  scan-time <milliseconds>
  scanning
  voip-aware-scan
```

Description

This command configures the Adaptive Radio Management (ARM) profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`40MHz-allowed-bands`	The specified setting allows ARM to determine if 40 MHz mode of operation is allowed on the 5 GHz or 2.4 GHz frequency band only, on both frequency bands, or on neither frequency band.	All/None/ a-only/g-only	a-only
`All`	Allows 40 MHz channels on both the 5 GHZ (802.11a) and 2.4 GHZ (802.11b/g) frequency bands.		
`None`	Disallows use of 40 MHz channels.		
`a-only`	Allows use of 40 MHz channels on the 5 GHZ (802.11a) frequency band only.		
`g-only`	Allows use of 40 MHz channels on the 2.4 GHZ (802.11b/g) frequency band only.		
`acceptable-coverage-index`	The minimal coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be. **NOTE:** This setting applies to multi-band implementations only.	1-6	4
`active-scan`	This parameter is intended for use in a lab environment only and is not a released feature. Do not use this parameter without proper guidance from Alcatel-Lucent.	Not intended for use.	Not intended for use.

assignment	Activates one of four ARM channel/power assignment modes.	—	single-band (new installations only)
disable	Disables ARM channel/power assignments.		
maintain	Maintains existing channel assignments.		
multi-band	Computes ARM assignments for both 5 GHZ (802.11a) and 2.4 GHZ (802.11b/g) frequency bands.		
single-band	Computes ARM assignments for a single band.		
backoff-time	Time, in seconds, an AP backs off after requesting a new channel or power.	120-3600	240 seconds
client-aware	When enabled, the AP does not change channels when there are active clients.	—	enabled
clone	Name of an existing ARM profile from which parameter values are copied.	—	—
error-rate-threshold	The percentage of errors in the channel that triggers a channel change. Recommended value is 50%.	0-100	50%
error-rate-wait-time	Time, in seconds, that the error rate has to be at least the error rate threshold to trigger a channel change.	1-2,147,483,647 Recommended Values: 1-100	30 seconds
free-channel-index	The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel. Recommended value is 25.	10-40	25
ideal-coverage-index	The coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be. Recommended value is 10.	2-20	10
load-aware-scan-threshold	This parameter is intended for use in a lab environment only and is not a released feature. Do not use this parameter without proper guidance from Alcatel-Lucent.	Not intended for use.	Not intended for use.
max-tx-power	Maximum effective isotropic radiated power (EIRP) from 0 to 30 dBm in 3 dBm increments. This value takes into account both radio transmit power and antenna gain. **NOTE:** Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30	30 dBm
min-scan-time	Time, in seconds, that a channel must be scanned before it is considered for assignment.	1-2,147,483,647 Recommended Values: 1-20	8 seconds
min-tx-power	Minimum effective isotropic radiated power (EIRP) from 0 to 30 dBm in 3 dBm increments. This value takes into account both radio transmit power and antenna gain. **NOTE:** Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30	9 dBm
mode-aware	This parameter is intended for use in a lab environment only and is not a released feature. Do not use this parameter without proper guidance from Alcatel-Lucent.	Not intended for use.	Not intended for use.
multi-band-scan	When enabled, single-radio APs try to scan across bands for rogue AP detection.	—	enabled
no	Negates any configured parameter.	—	—

noise-threshold	Maximum level of noise in a channel that triggers a channel change (-dBm).	0-2,147,483,647 Recommended Values: 0-80 -dBm	75 -dBm
noise-wait-time	Time, in seconds, the noise has to be high to trigger a channel change.	120-3600	120 seconds
ps-aware-scan	When enabled, the AP will not scan if Power Save is active.	—	enabled
rogue-ap-aware	When enabled, the AP will try to contain off-channel rogue APs.	—	disabled
scan-interval	Interval, in seconds, to drift out of the current channel.	0-2,147,483,647 Recommended Values: 0-30	10 seconds
scan-time	Duration, in milliseconds, to drift out of the current channel. The minimum value is 50 milliseconds.	50-2,147,483,647 Recommended Values: 50-200	110 milliseconds
scanning	Enables or disables AP scanning of other channels.	—	enabled
voip-aware-scan	When enabled, the AP will not scan if a VoIP call is in progress.	—	disabled

Usage Guidelines

Adaptive Radio Management (ARM) is a radio frequency (RF) resource allocation algorithm that allows each OmniAccess AP to determine the optimum channel selection and transmit power setting to minimize interference and maximize coverage and throughput. This command configures an ARM profile that you apply to a radio profile for the 5 GHz or 2.4 GHz frequency band (see “rf dot11a-radio-profile” on page 323 or “rf dot11g-radio-profile” on page 326).

If you were running an earlier version of AOS-W with ARM disabled, ARM remains disabled when you upgrade to the current release.

NOTE: AP configuration settings related to the IEEE 802.11n draft standard are configurable for Alcatel-Lucent’s OAW-AP120 series access points, which are IEEE 802.11n draft standard compliant devices.

Example

The following command configures VoIP-aware scanning for the arm-profile named “voice-arm:”

```
rf arm-profile voice-arm
  voip-aware-scan
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

Support for the high-throughput IEEE 802.11n draft standard was introduced in AOS-W 3.3.

The parameters active-scan, mode-aware, and load-aware-scan-threshold are not released features and were introduced in AOS-W 3.3.2 for intended use in a lab environment only. Do not use these parameters without proper guidance from Alcatel-Lucent.

Support for the wait-time parameter was removed in AOS-W 3.3.2.

rf dot11a-radio-profile

```
rf dot11a-radio-profile <profile>
  arm-profile <profile>
  beacon-period <milliseconds>
  channel <num|num+|num->
  clone <profile>
  csa
  csa-count <number>
  dot11h
  high-throughput-enable
  ht-radio-profile <profile>
  mgmt-frame-throttle-interval <seconds>
  mgmt-frame-throttle-limit <number>
  mode {ap-mode|am-mode|apm-mode|sensor-mode}
  no ...
  radio-enable
  tx-power <dBm>
```

Description

This command configures AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`arm-profile`	Configures Adaptive Radio Management (ARM) feature. See "rf arm-profile" on page 319.	—	"default"
`beacon-period`	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.	60 (minimum)	100 milliseconds
`channel`	Channel number for the AP 802.11a/802.11n physical layer. The available channels depend on the regulatory domain (country). Channel number configuration options for 20 MHz and 40 MHz modes: ■ num: Entering a channel number disables 40 MHz mode and activates 20 MHz mode for the entered channel. ■ num+: Entering a channel number with a plus (+) sign selects a primary and secondary channel for 40 MHz mode. The number entered becomes the primary channel and the secondary channel is determined by increasing the primary channel number by 4. Example: 157+ represents 157 as the primary channel and 161 as the secondary channel. ■ num-: Entering a channel number with a minus (-) sign selects a primary and secondary channel for 40 MHz mode. The number entered becomes the primary channel and the secondary channel is determined by decreasing the primary channel number by 4. Example: 157- represents 157 as the primary channel and 153 as the secondary channel. **NOTE:** 20 MHz clients are allowed to associate when a primary and secondary channel are configured; however, the client will only utilize the primary channel.	Depends on regulatory domain	—

clone	Name of an existing radio profile from which parameter values are copied.	—	—
csa	Channel Switch Announcement (CSA), as defined by IEEE 802.11h, allows an AP to announce that it is switching to a new channel before it begins transmitting on that channel. Clients must support CSA in order to track the channel change without experiencing disruption.	—	disabled
csa-count	Number of CSA announcements that are sent before the AP begins transmitting on the new channel.	1-16	4
dot11h	Enables 802.11h capability.	—	enabled
high-throughput-enable	Enables high-throughput (802.11n) features on the 5 GHz frequency band.	—	enabled
ht-radio-profile	Name of high-throughput radio profile to use for configuring high-throughput support on the 5 GHz frequency band. See "rf ht-radio-profile" on page 333.	—	"default-a"
mgmt-frame-throttle-interval	Averaging interval for rate limiting management frames in seconds. Zero disables rate limiting. Note: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.	0-60	1 second interval
mgmt-frame-throttle-limit	Maximum number of management frames allowed in each throttle interval. Note: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.	0-999999	20 frames per interval
mode	One of the operating modes for the AP.	ap-mode | am-mode | sensor-mode	ap-mode
ap-mode	Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN.		
am-mode	Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.		
apm-mode	This parameter is intended for use in a lab environment only and is not a released feature. Do not use this parameter without proper guidance from Alcatel-Lucent.	Not intended for use.	Not intended for use.
sensor-mode	Device operates as an RFprotect managed sensor. **NOTE:** Changing the mode of a radio from ap-mode or am-mode to sensor-mode or from sensor-mode to ap-mode or am-mode causes the AP to reboot. **NOTE:** For a dual-radio AP, setting one radio in sensor-mode causes both radios to behave as sensors.		
no	Negates any configured parameter.	—	—
radio-enable	Enables or disables radio configuration.	—	enabled
tx-power	Sets the initial transmit power (dBm) on which the AP operates, unless a better choice is available through either calibration or from RF Plan. Enter the value in .5 dBm increments.	0-30	14 dBm

Usage Guidelines

This command configures radios that operate in the 5 GHz frequency band, which includes radios utilizing the IEEE 802.11a or IEEE 802.11n draft standard. Channels must be valid for the country configured in the AP regulatory domain profile (see “ap regulatory-domain-profile” on page 77).

To view the supported channels, use the **show ap allowed-channels** command.

NOTE: AP configuration settings related to the IEEE 802.11n draft standard are configurable for Alcatel-Lucent’s OAW-AP120 series access points, which are IEEE 802.11n draft standard compliant devices.

Examples

The following command configures APs to operate in AM mode for the selected dot11a-radio-profile named “samplea:”

```
rf dot11a-radio-profile samplea
  mode am-mode
```

The following command configures APs to operate in high-throughput (802.11n) mode on the 5 Ghz frequency band for the selected dot11a-radio profile named “samplea” and assigns a high-throughout radio profile named “default-a:”

```
rf dot11a-radio-profile samplea
  high-throughput-enable
  ht-radio-profile default-a
```

The following command configures a primary channel number of 157 and a secondary channel number of 161 for 40 MHz mode of operation for the selected dot11a-radio profile named “samplea:”

```
rf dot11a-radio-profile samplea
  channel <157+>
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

Support for the high-throughput IEEE 802.11n draft standard was introduced in AOS-W 3.3.

Support for sensor-mode was introduced in AOS-W 3.3.2.

The apm-mode parameter is not a released feature and was introduced in AOS-W 3.3.2 for intended use in a lab environment only. Do not use apm-mode without proper guidance from Alcatel-Lucent.

rf dot11g-radio-profile

```
rf radio-profile <profile>
  arm-profile <profile>
  beacon-period <milliseconds>
  channel <num|num+|num->
  clone <profile>
  csa
  csa-count <number>
  dot11h
  dot11b-protection
  high-throughput-enable
  ht-radio-profile <profile>
  mgmt-frame-throttle-interval <seconds>
  mgmt-frame-throttle-limit <number>
  mode {ap-mode|am-mode|apm-mode|sensor-mode}
  no ...
  radio-enable
  tx-power <dBm>
```

Description

This command configures AP radio settings for the 2.4 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`arm-profile`	Configures Adaptive Radio Management (ARM) feature. See "rf arm-profile" on page 319.	—	"default"
`beacon-period`	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.	60 (minimum)	100 milliseconds

`channel`	Channel number for the AP 802.11g/802.11n physical layer. The available channels depend on the regulatory domain (country). Channel number configuration options for 20 MHz and 40 MHz modes: ■ num: Entering a channel number disables 40 MHz mode and activates 20 MHz mode for the entered channel. ■ num+: Entering a channel number with a plus (+) sign selects a primary and secondary channel for 40 MHz mode. The number entered becomes the primary channel and the secondary channel is determined by increasing the primary channel number by 4. Example: 1+ represents 1 as the primary channel and 5 as the secondary channel. ■ num-: Entering a channel number with a minus (-) sign selects a primary and secondary channel for 40 MHz mode. The number entered becomes the primary channel and the secondary channel is determined by decreasing the primary channel number by 4. Example: 5- represents 5 as the primary channel and 1 as the secondary channel. **NOTE:** 20 MHz clients are allowed to associate when a primary and secondary channel are configured; however, the client will only utilize the primary channel.	Depends on regulatory domain	—
`clone`	Name of an existing radio profile from which parameter values are copied.	—	—
`csa`	Channel Switch Announcement (CSA), as defined by IEEE 802.11h, allows an AP to announce that it is switching to a new channel before it begins transmitting on that channel. Clients must support CSA in order to track the channel change without experiencing disruption.	—	disabled
`csa-count`	Number of CSA announcements that are sent before the AP begins transmitting on the new channel.	1-16	4
`dot11h`	Enables 802.11h capability.	—	enabled
`dot11b-protection`	Enables or disables protection for 802.11b clients. The protection status is displayed in the output of `show ap details` and `show ap active` commands of the APs local WLAN switch.		enabled
`high-throughput-enable`	Enables high-throughput (802.11n) features on the 2.4 GHz frequency band.	—	enabled
`ht-radio-profile`	Name of high-throughput radio profile to use for configuring high-throughput support on the 2.4 GHz frequency band. See "rf ht-radio-profile" on page 333.	—	"default-g"
`mgmt-frame-throttle-interval`	Averaging interval for rate limiting management frames in seconds. Zero disables rate limiting. Note: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.	0-60	1 second interval
`mgmt-frame-throttle-limit`	Maximum number of management frames allowed in each throttle interval. Note: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.	0-999999	20 frames per interval
`mode`	One of the operating modes for the AP.	ap-mode | am-mode | sensor-mode	ap-mode

ap-mode	Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN.		
am-mode	Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.		
apm-mode	This parameter is intended for use in a lab environment only and is not a released feature. Do not use this parameter without proper guidance from Alcatel-Lucent.	Not intended for use.	Not intended for use.
sensor-mode	Device operates as an RFprotect managed sensor. **NOTE:** Changing the mode of a radio from ap-mode or am-mode to sensor-mode or from sensor-mode to ap-mode or am-mode causes the AP to reboot. **NOTE:** For a dual-radio AP, setting one radio in sensor-mode causes both radios to behave as sensors.		
no	Negates any configured parameter.	—	—
radio-enable	Enables or disables radio configuration.	—	enabled
tx-power	Sets the initial transmit power (dBm) on which the AP operates, unless a better choice is available through either calibration or from RF Plan. Enter the value in .5 dBm increments.	0-30	14 dBm

Usage Guidelines

This command configures radios that operate in the 2.4 GHz frequency band, which includes radios utilizing the IEEE 802.11b/g or IEEE 802.11n draft standard. Channels must be valid for the country configured in the AP regulatory domain profile (see "ap regulatory-domain-profile" on page 77).

To view the supported channels, use the **show ap allowed-channels** command.

NOTE: AP configuration settings related to the IEEE 802.11n draft standard are configurable for Alcatel-Lucent's OAW-AP120 series access points, which are IEEE 802.11n draft standard compliant devices.

Examples

The following command configures APs to operate in AM mode for the selected dot11g-radio-profile named "sampleg:"

```
rf dot11g-radio-profile sampleg
  mode am-mode
```

The following command configures APs to operate in high-throughput (802.11n) mode on the 2.4 Ghz frequency band for the selected dot11g-radio profile named "sampleg" and assigns a high-throughout radio profile named "default-g:"

```
rf dot11g-radio-profile sampleg
  high-throughput-enable
  ht-radio-profile default-g
```

The following command configures a primary channel number of 1 and a secondary channel number of 5 for 40 MHz mode of operation for the selected dot11g-radio profile named “sampleg:”

```
rf dot11g-radio-profile sampleg
   channel <1+>
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

Support for the high-throughput IEEE 802.11n draft standard was introduced in AOS-W 3.3.

Support for sensor-mode was introduced in AOS-W 3.3.2.

The apm-mode parameter is not a released feature and was introduced in AOS-W 3.3.2 for intended use in a lab environment only. Do not use apm-mode without proper guidance from Alcatel-Lucent.

Support for the dot11b-protection parameter was introduced in AOS-W 3.3.2.

rf event-thresholds-profile

```
rf event-thresholds-profile <profile>
  bwr-high-wm <percent>
  bwr-low-wm <percent>
  clone <profile>
  detect-frame-rate-anomalies
  fer-high-wm <percent>
  fer-low-wm <percent>
  ffr-high-wm <percent>
  ffr-low-wm <percent>
  flsr-high-wm <percent>
  flsr-low-wm <percent>
  fnur-high-wm <percent>
  fnur-low-wm <percent>
  frer-high-wm <percent>
  frer-low-wm <percent>
  frr-high-wm <percent>
  frr-low-wm <percent>
  no ...
```

Description

This command configures the event thresholds profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`bwr-high-wm`	If bandwidth in an AP exceeds this value, a bandwidth exceeded condition exists. The value represents the percentage of maximum for a given radio. (For 802.11b, the maximum bandwidth is 7 Mbps. For 802.11 a and g, the maximum is 30 Mbps.) The recommended value is 85%.	0-100	0%
`bwr-low-wm`	After a bandwidth exceeded condition exists, the condition persists until bandwidth drops below this value. The recommended value is 70%.	0-100	0%
`clone`	Name of an existing radio profile from which parameter values are copied.	—	—
`detect-frame-rate-anomalies`	Enable or disables detection of frame rate anomalies.	—	disabled
`fer-high-wm`	If the frame error rate (as a percentage of total frames in an AP) exceeds this value, a frame error rate exceeded condition exists. The recommended value is 16%.	0-100	0%
`fer-low-wm`	After a frame error rate exceeded condition exists, the condition persists until the frame error rate drops below this value. The recommended value is 8%.	0-100	0%
`ffr-high-wm`	If the frame fragmentation rate (as a percentage of total frames in an AP) exceeds this value, a frame fragmentation rate exceeded condition exists. The recommended value is 16%.	0-100	16%
`ffr-low-wm`	After a frame fragmentation rate exceeded condition exists, the condition persists until the frame fragmentation rate drops below this value. The recommended value is 8%.	0-100	8%

`flsr-high-wm`	If the rate of low-speed frames (as a percentage of total frames in an AP) exceeds this value, a low-speed rate exceeded condition exists. This could indicate a coverage hole. The recommended value is 16%.	0-100	16%
`flsr-low-wm`	After a low-speed rate exceeded condition exists, the condition persists until the percentage of low-speed frames drops below this value. The recommended value is 8%.	0-100	8%
`fnur-high-wm`	If the non-unicast rate (as a percentage of total frames in an AP) exceeds this value, a non-unicast rate exceeded condition exists. This value depends upon the applications used on the network.	0-100	0%
`fnur-low-wm`	After a non-unicast rate exceeded condition exists, the condition persists until the non-unicast rate drops below this value.	0-100	0%
`frer-high-wm`	If the frame receive error rate (as a percentage of total frames in an AP) exceeds this value, a frame receive error rate exceeded condition exists. The recommended value is 16%.	0-100	16%
`frer-low-wm`	After a frame receive error rate exceeded condition exists, the condition persists until the frame receive error rate drops below this value. The recommended value is 8%.	0-100	8%
`frr-high-wm`	If the frame retry rate (as a percentage of total frames in an AP) exceeds this value, a frame retry rate exceeded condition exists. The recommended value is 16%.	0-100	16%
`frr-low-wm`	After a frame retry rate exceeded condition exists, the condition persists until the frame retry rate drops below this value. The recommended value is 8%.	0-100	8%
`no`	Negates any configured parameter.	—	—

Usage Guidelines

The event threshold profile configures Received Signal Strength Indication (RSSI) metrics. When certain RF parameters are exceeded, these events can signal excessive load on the network, excessive interference, or faulty equipment. This profile and many of the detection parameters are disabled (value is 0) by default.

Example

The following command configures an event threshold profile:

```
rf event-thresholds-profile et1
   detect-frame-rate-anomalies
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

rf ht-radio-profile

```
rf ht-radio-profile <profile>
  40MHz-intolerance
  clone <profile>
  honor-40MHz-intolerance
  no
```

Description

This command configures high-throughput AP radio settings. High-throughput features utilize the IEEE 802.11n draft standard.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters. **Default Options:** "Default-a" is generally used in association with high-throughput devices running on the 5 GHz frequency band, see "rf dot11a-radio-profile" on page 323. "Default-g" is generally used in association with high-throughput devices running on the 2.4 GHz frequency band, see "rf dot11g-radio-profile" on page 326. "Default" is generally used when the same ht-radio-profile is desired for use with both frequency bands.	—	"default-a" "default-g" "default"
`40MHz-intolerance`	Controls whether or not APs using this radio profile will advertise intolerance of 40 MHz operation. By default, 40 MHz operation is allowed.	—	disabled
`clone`	Name of an existing high-throughput radio profile from which parameter values are copied.	—	—
`honor-40MHz-intolerance`	When enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.	—	enabled
`no`	Negates any configured parameter.	—	—

Usage Guidelines

The ht-radio-profile configures high-throughput settings for networks utilizing the IEEE 802.11n draft standard, which supports 40 MHZ channels and operates in both the 2.4 GHZ and 5 GHZ frequency bands.

The ht-radio-profile you wish to use must be assigned to a dot11a and/or dot11g-radio-profile. You can assign the same profile or different profiles to the 2.4 GHZ and 5 GHZ frequency bands. See "rf dot11a-radio-profile" on page 323 and "rf dot11g-radio-profile" on page 326.

NOTE: AP configuration settings related to the IEEE 802.11n draft standard are configurable for Alcatel-Lucent's OAW-AP120 series access points, which are IEEE 802.11n draft standard compliant devices.

Example

The following command configures an ht-radio-profile named “default-g” and enables 40MHz-intolerance:

```
rf ht-radio-profile default-g
  40MHz-intolerance
```

Platform Availability

This command is available on all platforms but operates with IEEE 802.11n compliant devices only.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.3.

Support for the dsss-cck-40mhz parameter was removed in AOS-W 3.3.2.

rf optimization-profile

```
rf optimization-profile <profile>
  ap-lb-max-retries <number>
  ap-lb-user-high-wm <percent>
  ap-lb-user-low-wm <percent>
  ap-lb-util-high-wm <percent>
  ap-lb-util-low-wm <percent>
  ap-lb-util-wait-time <seconds
  ap-load-balancing
  clone <profile>
  coverage-hole-detection
  detect-association-failure
  detect-interference
  handoff-assist
  hole-detection-interval <seconds>
  hole-good-rssi-threshold <number>
  hole-good-sta-ageout <seconds>
  hole-idle-sta-ageout <seconds>
  hole-poor-rssi-threshold <number>
  interference-baseline <seconds>
  interference-exceed-threshold <seconds>
  interference-threshold <percent>
  low-rssi-threshold <number>
  no ...
  rssi-check-frequency <number>
  rssi-falloff-wait-time <seconds>
```

Description

This command configures the RF optimization profile.

Syntax

Parameter	Description	Range	Default
<profile>	Name of this instance of the profile. The name must be 1-63 characters.	—	“default”
ap-lb-max-retries	When load balancing is enabled, this is the maximum number of times a new station is encouraged to move to another AP. If the station still attempts to associate with the AP after that, association is allowed.		8
ap-lb-user-high-wm	When load balancing is enabled, reaching or exceeding the high watermark value triggers load balancing. Load balancing stops when the low watermark value is reached.		0
ap-lb-user-low-wm	When load balancing is enabled, reaching or exceeding the high watermark value triggers load balancing. Load balancing stops when the low watermark value is reached.		0
ap-lb-util-high-wm	When load balancing is enabled, reaching or exceeding the high watermark value triggers load balancing. Load balancing stops when the low watermark value is reached.		0
ap-lb-util-low-wm	When load balancing is enabled, reaching or exceeding the high watermark value triggers load balancing. Load balancing stops when the low watermark value is reached.		0
ap-lb-util-wait-time	Time, in seconds, to wait before starting or stopping load balancing once a watermark value is reached.		0 seconds

ap-load-balancing	Allows system to balance wireless traffic across APs in the AP group. Load balancing can be triggered based on the number of users or degree of utilization on an AP. When traffic reaches configured thresholds on an AP where load balancing is enabled, any new wireless client station attempting to associate with the AP will be directed to another AP in the group.	—	disabled
clone	Name of an existing optimization profile from which parameter values are copied.	—	—
coverage-hole-detection	Enables or disables coverage hole detection. **NOTE:** The Wireless Intrusion Protection license must be installed.	—	disabled
detect-association-failure	Enables or disables STA association failure detection.	—	disabled
detect-interference	Enables or disables interference detection.	—	disabled
handoff-assist	Allows the WLAN switch to force a client off an AP when the RSSI drops below a defined minimum threshold.	—	disabled
hole-detection-interval	Time, in seconds, after a coverage hole is detected until a coverage hole event notification is generated. **NOTE:** The Wireless Intrusion Protection license must be installed.		180 seconds
hole-good-rssi-threshold	Stations with signal strength above this value are considered to have good coverage. **NOTE:** The Wireless Intrusion Protection license must be installed.		20
hole-good-sta-ageout	Time, in seconds, after which a station with good coverage is aged out. **NOTE:** The Wireless Intrusion Protection license must be installed.		30 seconds
hole-idle-sta-ageout	Time, in seconds, after which a station in a poor coverage area is aged out. **NOTE:** The Wireless Intrusion Protection license must be installed.		90 seconds
hole-poor-rssi-threshold	Stations with signal strength below this value will trigger detection of a coverage hole. **NOTE:** The Wireless Intrusion Protection license must be installed.		10
interference-baseline	Time, in seconds, the air monitor should learn the state of the link between the AP and client to create frame retry rate (FRR) and frame receive error rate (FRER) baselines.		30 seconds
interference-exceed-time	Time, in seconds, the FRR or FRER exceeds the threshold before interference is reported.		30 seconds
interference-threshold	Percentage increase in the frame retry rate (FRR) or frame receive error rate (FRER) before interference monitoring begins on a given channel.	0-100	100%
low-rssi-threshold	Minimum RSSI, above which deauth should never be sent.		0
no	Negates any configured parameter.	—	—
rssi-check-frequency	Interval, in seconds, to sample RSSI.		0 seconds

`rssi-falloff-wait-time`	Time, in seconds, to wait with decreasing RSSI before deauth is sent to the client. The maximum value is 8 seconds.	0-8	0 seconds

Usage Guidelines

The RF optimization includes parameters for the following features:

- AP load balancing.
- Coverage hole detection looks for clients unable to associate to any AP or clients that are associating at very low data rates or with low signal strength. These symptoms indicate areas where holes in radio coverage exist. When the system detects such coverage holes, you are notified of the condition via the event log.
- Detection of interference near a wireless client station or AP based on an increase in the frame retry rate or frame receive error rate.

Example

The following command configures an RF optimization profile:

```
rf optimization-profile opt1
  coverage-hole-detection
  detect-association-failure
  detect-interference
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for the noted parameters.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.0.

rft

```
rft test profile antenna-connectivity ap-name <name> [dest-mac <macaddr> [phy {a|g}|
 radio {0|1}]]

rft test profile link-quality {ap-name <name> dest-mac <macaddr> [phy {a|g}|
 radio {0|1}] | bssid <bssid> dest-mac <macaddr> | ip-addr <ipaddr>
 dest-mac <macaddr> [phy {a|g}|radio {0|1}]}

rft test profile raw {ap-name <name> dest-mac <macaddr> [phy {a|g}|radio {0|1}] | bssid
 <bssid> dest-mac <macaddr> | ip-addr <ipaddr> dest-mac <macaddr> [phy {a|g}|radio
 {0|1}]}
```

Description

This command is used for RF troubleshooting.

Syntax

Parameter	Description	Range	Default
`ap-name`	Name of the AP that performs the test.	—	—
`dest-mac`	MAC address of the client to be tested.	—	—
`phy`	802.11 type, either a or g.	a | g	—
`radio`	Radio ID, either 0 or 1.	0 | 1	—
`bssid`	BSSID of the AP that performs the test.	—	—
`ip-addr`	IP address of the AP that performs the test.		

Usage Guidelines

This command can run predefined test profiles for antenna connectivity, link quality, or raw testing.

NOTE: You should only run these commands when directed to do so by an Alcatel-Lucent support representative.

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on the master WLAN switch.

History

This command was available in AOS-W 3.0.

router

```
router mobile
```

Description

This command enables Layer-3 (IP) mobility.

Syntax

No parameters.

Usage Guidelines

IP mobility is disabled by default on the WLAN switch. You need to use this command to enable IP mobility. This command must be executed on all WLAN switches (master and local) that need to provide support for layer-3 roaming in a mobility domain.

You can disable IP mobility in a virtual AP profile with the **wlan virtual-ap** command (IP mobility is enabled by default in a virtual AP profile).

Example

This command enables IP mobility:

```
router mobile
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

service

```
service dhcp
```

Description

This command enables the DHCP server on the WLAN switch.

Syntax

Parameter	Description	Range	Default
`dhcp`	Enables the DHCP server.	—	disabled

Usage Guidelines

You can enable and configure the DHCP server in the WLAN switch to provide IP addresses to wireless clients if an external DHCP server is not available.

Use the **ip dhcp** commands to configure the IP address pools used by the DHCP server.

Example

The following command enables the DHCP server in the WLAN switch:

```
service dhcp
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

shutdown

```
shutdown all
```

Description

This command disables all interfaces on the WLAN switch.

Usage Guidelines

This command stops all traffic through the physical ports on the WLAN switch. The console port remains active. Use this command only when you have physical access to the WLAN switch, so that you can continue to manage using the console port.

To shut down an individual interface, tunnel, or VLAN, use the `shutdown` option within the `interface` command.

To restore the ports, use the `no shutdown` command.

Example

The following example shuts down all physical interfaces on the WLAN switch.

```
shutdown all
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 1.0.

snmp-server

```
snmp-server community <string>|enable trap|
host <ipaddr> version {1 <name> udp-port <port>}|{2c|3 <name> [inform]
 [interval <seconds>] [retrycount <number>] [udp-port <port>]}|
inform queue-length <size>|stats|trap source <ipaddr>|
user <name> [auth-prot {md5|sha} <password>] [priv-prot {AES|DES} <password>]
```

Description

This command configures SNMP parameters.

Syntax

Parameter	Description	Range	Default
`community`	Sets the read-only community string.	—	—
`enable trap`	Enables sending of SNMP traps to the configured host.	—	disabled
`host`	Configures the IP address of the host to which SNMP traps are sent. This host needs to be running a trap receiver to receive and interpret the traps sent by the WLAN switch.	—	—
`version`	Configures the SNMP version and security string for notification messages.	—	—
`inform`	Sends SNMP inform messages to the configured host.	—	disabled
`interval`	Estimated round trip time to this host.		60 seconds
`retrycount`	Number of times that SNMP inform messages are attempted to be sent to the host before giving up.		3
`udp-port`	The port number to which notification messages are sent.	—	162
`stats`	Allows file-based statistics collection for OV-MM. The WLAN switch generates a file that contains statistics data used by OV-MM to display information in chart and graph formats. File-based statistics collection is transparent to the user and increases the efficiency of transferring information between the WLAN switch and OV-MM.		enabled
`inform`	Specifies the length for the SNMP inform queue.	100-350	250
`trap`	Source IP address of SNMP traps.	—	disabled
`disable`	Disables an SNMP trap. You can get a list of valid trap names using the `show snmp trap-list` command.	—	—
`enable`	Enables an SNMP trap.	—	—
`source`	The IP address of the destination to which the trap is sent.	—	—
`user`	Configures an SNMPv3 user profile for the specified username.	—	—
`auth-prot`	Authentication protocol for the user, either HMAC-MD5-98 Digest Authentication Protocol (MD5) or HMAC-SHA-98 Digest Authentication Protocol (SHA), and the password for use with the designated protocol.	MD5/SHA	SHA
`priv-prot`	Privacy protocol for the user, either Advanced Encryption Standard (AES) or CBC-DES Symmetric Encryption Protocol (DES), and the password for use with the designated protocol.	AES/DES	DES

Usage Guidelines

This command configures SNMP on the WLAN switch only. You configure SNMP-related information for APs in an SNMP profile which you apply to an AP group or to a specific AP. To configure SNMP hostname, contact, and location information for the WLAN switch, use the hostname, syscontact, and syslocation commands.

Example

The following command configures an SNMP trap receiver:

```
snmp-server host 191.168.1.1 version 2c 12345678
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

The stats parameter was introduced in AOS-W 3.3.1.

spanning-tree

```
spanning-tree
  [forward-time <value> | hello-time <value> | max-age <value> | priority <value>]
```

Description

This command configures the Spanning Tree Protocol (STP).

Syntax

Parameter	Description	Range	Default
`forward-time`	Specifies the time, in seconds, the port spends in the listening and learning state. During this time, the port waits to forward data packets.	4-30	15 seconds
`hello-time`	Specifies the time, in seconds, between each bridge protocol data unit (BPDU) transmitted by the root bridge.	1-10	2 seconds
`max-age`	Specifies the time, in seconds, the root bridge waits to receive a hello packet before changing the STP topology.	6-40	20 seconds
`priority`	Set the priority of a bridge to make it more or less likely to become the root bridge. The bridge with the lowest value has the highest priority. When configuring the priority, remember the following: ■ The highest priority bridge is the root bridge. ■ The highest priority value is 0 (zero).	0-65535	32768

Usage Guidelines

This command configures the STP settings on the WLAN switch.

By default, all ports on the WLAN switch are running default 802.1D spanning tree on VLAN 1 and STP is enabled. The default STP parameters can be left for most implementations.

Use the `no spanning-tree` command to disable STP.

Example

The following command sets the time a port spends in the listening and learning state to 3 seconds:

```
spanning-tree forward-time 3
```

The following command sets the time the root bridge waits to transmit BPDUs to 4 seconds:

```
spanning-tree hello-time 4
```

The following command sets the time the root bridge waits to receive a hello packet to 30 seconds:

```
spanning-tree max-age 30
```

The following command sets the bridge priority to 10, making it more likely to become the root bridge:

```
spanning-tree priority 10
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 1.0.

ssh

```
ssh disable_dsa | mgmt-auth {public-key [username/password] | username/password
[public-key]}
```

Description

This command configures SSH access to the WLAN switch.

Syntax

Parameter	Description	Range	Default
`disable_dsa`	Disables DSA authentication for SSH. Only RSA authentication is used.	—	—
`mgmt-auth`	Configures authentication method for the management user. You can specify username/password only, public key only, or both username/password and public key.	—	username/ password

Usage Guidelines

Public key authentication is supported using a X.509 certificate issued to the management client. If you specify public-key authentication, you need to load the client X.509 certificate into the WLAN switch and configure certificate authentication for the management user with the mgmt-user ssh-pubkey command.

Example

The following commands configure SSH access using public key authentication only:

```
ssh mgmt-auth public-key
mgmt-user ssh-pubkey client-cert ssh-pubkey cli-admin root
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

The mgmt-auth parameter was introduced in AOS-W 3.1.

stm

```
stm add-blacklist-client <macaddr> | kick-off-sta <macaddr> <bssid>|
remove-blacklist-client <macaddr> | start-trace <macaddr> | stop-trace <macaddr>
```

Description

This command is used to manually control the blacklisting of clients.

Syntax

Parameter	Description	Range	Default
`add-blacklist-client`	MAC address of the client to be added to the denial of service list.	—	—
`kick-off-sta`	MAC address of the client to disassociated.	—	—
`<bssid>`	AP from which the client is to be kicked off.	—	—
`remove-blacklist-client`	MAC address of the client to remove from the denial of service list.	—	—
`start-trace`	Client or BSSID on which to start tracing.	—	—
`stop-trace`	Client or BSSID on which to stop tracing.	—	—

Usage Guidelines

When you blacklist a client, the client is not allowed to associate with any AP in the network. If the client is connected to the network when you blacklist it, a deauthentication message is sent to force the client to disconnect. The blacklisted client is blacklisted for the duration specified in the virtual AP profile.

Example

The following command blacklists a client:

```
stm add-blacklist-client 00:01:6C:CC:8A:6D
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

support

```
support
```

Description

This command, which should be used only in conjunction with Alcatel-Lucent customer support, is for WLAN switch debugging purposes only.

Syntax

No parameters.

Usage Guidelines

NOTE: Use this command only under the guidance of Alcatel-Lucent customer support.

This command is used by Alcatel-Lucent customer support for debugging the WLAN switch. Do not use this command without the guidance of Alcatel-Lucent customer support.

In AOS-W 2.4 and 2.5, this command was named `secret`.

Example

The following command allows Alcatel-Lucent customer support to debug the WLAN switch:

```
support
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode.

History

This command was available as the `secret` command in AOS-W 2.4.

This command was renamed to `support` in AOS-W 3.1.

syscontact

```
syscontact <syscontact>
```

Description

This command configures the name of the system contact for the WLAN switch.

Syntax

Parameter	Description	Range	Default
`syscontact`	An alphanumeric string that specifies the name of the system contact.	—	—

Usage Guidelines

Use this command to enter the name of the person who acts as the system contact or administrator for the WLAN switch. You can use a combination of numbers, letters, characters, and spaces to create the name. To include a space in the name, use quotation marks to enclose the alphanumeric string. For example, to create the system contact name Lab Technician 1, enter "`Lab Technician 1`" at the prompt.

To change the existing name, enter the command with a different string. The new name takes affect immediately. To unconfigure the name, enter "" at the prompt.

If you enter an unsupported attribute, the WLAN switch displays a message similar to the following:

```
% Invalid input detected at '^' marker.
```

Example

The following command defines LabTechnician as the system contact name:

```
syscontact LabTechnician
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 1.0.

syslocation

```
syslocation <string>
```

Description

This command configures the location of the WLAN switch.

Syntax

Parameter	Description	Range	Default
`syslocation`	A text string that specifies the system location.	—	—

Usage Guidelines

Use this command to indicate the location of the WLAN switch. You can use a combination of numbers, letters, characters, and spaces to create the name. To include a space in the name, use quotation marks to enclose the text string.

To change the existing name, enter the command with a different string. To unconfigure the location, enter "" at the prompt.

Example

The following command defines SalesLab as the location for the WLAN switch:

```
syslocation "Building 10, second floor, room 21E"
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

tar

```
tar clean {crash|flash|logs}| crash | flash | logs [tech-support]
```

Description

This command archives a directory.

Syntax

Parameter	Description	Range	Default
`clean`	Removes a tar file.	—	—
`crash`	Removes crash.tar.	—	—
`flash`	Removes flash.tar.gz.	—	—
`logs`	Removes logs.tar.	—	—
`crash`	Archives the crash directory to crash.tar. A crash directory must exist.	—	—
`flash`	Archives and compresses the /flash directory to flash.tar.gz.	—	—
`logs`	Archives the logs directory to log.tar. Optionally, technical support information can be included.	—	—

Usage Guidelines

This command creates archive files in Unix tar file format.

Example

The following command creates the log.tar file with technical support information:

```
tar logs tech-support
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

telnet

```
telnet {cli | soe}
```

Description

Enable telnet to the WLAN switch or to an AP through the WLAN switch.

Syntax

Parameter	Description	Range	Default
`cli`	Enable telnet using the CLI.	—	Disabled
`soe`	Enable telnet using Serial over Ethernet (SoE).	—	Disabled

Usage Guidelines

Use the `cli` option to enable telnet to the WLAN switch.

Use the `soe` option to enable telnet using the SoE protocol. This allows you to remotely manage an AP directly connected to the WLAN switch.

Example

The following example enables telnet to the WLAN switch using the CLI.

```
telnet cli
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was introduced in AOS-W 1.0.

time-range

```
time-range <name> absolute [end <mm/dd/yyyy> <hh:mm>]|[start <mm/dd/yyyy> <hh:mm>]
time-range <name> periodic
   Daily <hh:mm> to <hh:mm>
   Friday <hh:mm> to <hh:mm>
   Monday <hh:mm> to <hh:mm>
   Saturday <hh:mm> to <hh:mm>
   Sunday <hh:mm> to <hh:mm>
   Thursday <hh:mm> to <hh:mm>
   Tuesday <hh:mm> to <hh:mm>
   Wednesday <hh:mm> to <hh:mm>
   Weekday <hh:mm> to <hh:mm>
   Weekend <hh:mm> to <hh:mm>
   no ...
```

Description

This command configures time ranges.

Syntax

Parameter	Description	Range	Default
<name>	Name of this time range. You can reference this name in other commands.	—	—
absolute	Specifies an absolute time range, with a specific start and/or end time and date.	—	—
periodic	Specifies a recurring time range. Specify the start and end time and Daily, Weekday, Weekend, or the day of the week.	—	—
no	Negates any configured parameter.	—	—

Usage Guidelines

You can use time ranges when configuring session ACLs. Once you configure a time range, you can use it in multiple session ACLs.

Example

The following command configures a time range for daytime working hours:

```
time-range working-hours periodic
  weekday 7:30 to 18:00
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Policy Enforcement Firewall license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

traceroute

```
traceroute <ipaddr>
```

Description

Trace the route to the specified IP address.

Syntax

Parameter	Description	Range	Default
`ipaddr`	The destination IP address.	—	—

Usage Guidelines

Use this command to identify points of failure in your network.

Example

The following command traces the route to the device identified by the IP address 10.1.2.3.

```
traceroute 10.1.2.3
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in user, privileged, and config modes.

History

This command was available in AOS-W 2.0.

trusted

```
trusted all
```

Description

This command makes all physical interfaces on the WLAN switch trusted ports.

Syntax

Parameter	Description	Range	Default
`all`	Makes all ports on the WLAN switch trusted.	—	—

Usage Guidelines

Trusted ports are typically connected to internal controlled networks. Untrusted ports connect to third-party APs, public areas, or any other network to which the WLAN switch should provide access control. When OmniAccess APs are attached directly to the WLAN switch, set the connecting port to be trusted.

By default, all ports on the WLAN switch are treated as trusted. You can use the **interface fastethernet** or **interface gigabitethernet** commands to make individual ports trusted.

Example

The following command makes all ports trusted:

```
trusted all
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

user-role

```
user-role <name>
  access-list {eth|mac|session} <acl> [ap-group <group>] [position <number>]
  bw-contract <name> [per-user] {downstream|upstream}
  captive-portal <profile>
  dialer <name>
  max-sessions <number>
  no ...
  pool {l2tp|pptp} <name>
  reauthentication-interval <minutes>
  session-acl <acl> [ap-group <group>] [position <number>]
  vlan <id>
```

Description

This command configures a user role.

Syntax

Parameter	Description	Range	Default
`<name>`	Name of the user role.	—	—
`access-list`	Type of access control list (ACL) to be applied: ■ eth: Ethertype ACL configured with the **ip access-list eth** command. ■ mac: MAC ACL configured with the **ip access-list mac** command. ■ session: Session ACL configured with the **ip access-list session** command.	—	—
`<acl>`	Name of the configured ACL.		
`ap-group`	(Optional) AP group to which this ACL applies.	—	—
`position`	(Optional) Position of this ACL relative to other ACLs that you can configure for the user role. 1 is the top.	—	(last)
`bandwidth-contract`	Name of a bandwidth contract or rate limiting policy configured with the **aaa bandwidth-contract** command. The bandwidth contract must be applied to either downstream or upstream traffic.	—	—
`downstream`	Applies the bandwidth contract to traffic from the WLAN switch to the client.	—	—
`per-user`	Specifies that bandwidth contract is assigned on a per-user basis instead of a per-role basis. For example, if two users are active on the network and both are part of the same role with a 500 Kbps bandwidth contract, then each user is able to use up to 500 Kbps.	—	(per role)
`upstream`	Applies the bandwidth contract to traffic from the client to the WLAN switch.	—	—
`captive-portal`	Name of the captive portal profile configured with the **aaa authentication captive-portal** command.	—	—
`dialer`	If VPN is used as an access method, name of the VPN dialer configured with the **vpn-dialer** command. The user can login using captive portal and download the dialer. The dialer is a Windows application that configures the VPN client.	—	—
`max-sessions`	Maximum number of datapath sessions per user in this role.	0-65535	65535

no	Negates any configured parameter.	—	—
pool	If VPN is used as an access method, specifies the IP address pool from which the user's IP address is assigned: ■ l2tp: When a user negotiates a Layer-2 Tunneling Protocol (L2TP)/ IPSec session, specifies an address pool configured with the **ip local pool** command. ■ pptp: When a user negotiates a Point-to-Point Tunneling Protocol (PPTP) session, specifies an address pool configured with the **pptp ip local pool** command.	—	—
<name>	Name of the L2TP or PPTP pool to be applied.	—	—
reauthentication-interval	Interval, in minutes, after which the client is required to reauthenticate.	0-4096, 0 to disable	0 (disabled)
session-acl	Session ACL configured with the **ip access-list session** command.	—	—
ap-group	(Optional) AP group to which this ACL applies.	—	—
position	(Optional) Position of this ACL relative to other ACLs that you can configure for the user role. 1 is the top.	—	(last)
vlan	VLAN to which the user assigned this user role is mapped. This parameters works only when using Layer-2 authentication such as 802.1x or MAC address, ESSID, or encryption type role mapping because these authentications occur before an IP address is assigned. If a user authenticates using a Layer-3 mechanism such as VPN or captive portal this parameter has no effect.	—	—

Usage Guidelines

Every client in an Alcatel-Lucent user-centric network is associated with a user role. All wireless clients start in an initial role. From the initial role, clients can be placed into other user roles as they pass authentication.

Example

The following command configures a user role:

```
user-role new-user
  dialer default-dialer
  pool pptp-pool-1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Policy Enforcement Firewall license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

vlan

```
vlan <id> [<name>]
```

Description

This command creates a VLAN on the WLAN switch.

Syntax

Parameter	Description	Range	Default
`vlan`	Identification number for the VLAN.	2-4094	—
`<name>`	(Optional) Name for the VLAN.	—	VLAN<id>

Usage Guidelines

Use the **interface vlan** command to configure the VLAN interface, including an IP address.

Example

The following command creates a VLAN on the WLAN switch:

```
vlan 27
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

voip

```
voip [prioritization {disable|enable}]
```

Description

This command enables Voice over IP (VoIP) traffic prioritization.

Syntax

Parameter	Description	Range	Default
`prioritization`	Allows voice traffic to be assigned automatically to the high priority queue.	—	disabled

Usage Guidelines

This command allows VoIP traffic to be automatically assigned to the high-priority queue. When this command is enabled, you do not need to configure a session ACL to place voice traffic into the high-priority queue.

Example

The following command enables VoIP traffic prioritization:

```
voip prioritization
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Voice Services Module license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

vpdn group l2tp

```
vpdn group l2tp
  client configuration {dns|wins} <ipaddr1> [<ipaddr2>]
  disable|enable
  l2tp tunnel hello <seconds>
  no ...
  ppp authentication {CACHE-SECURID|CHAP|EAP|MSCHAP|MSCHAPv2|PAP}
  ppp securid cache <minutes>
```

Description

This command configures an L2TP/IPSec VPN connection.

Syntax

Parameter	Description	Range	Default
`client configuration`	Configures parameters for the remote clients.	—	—
`dns`	Configures a primary and optional secondary DNS server.	—	—
`wins`	Configures a primary and optional secondary WINS server.	—	—
`disable|enable`	Disables or enables termination of L2TP clients.	—	enabled
`l2tp tunnel hello`	Configures L2TP tunneling hello timeout, in seconds.	10-1440	60 seconds
`no`	Negates any configured parameter.	—	—
`ppp authentication`	Enables the protocols for PPP authentication. This list should match the L2TP configuration configured with the **vpn-dialer** command on the WLAN switch.	—	—
`CACHE-SECUR ID`	The WLAN switch caches Secure ID tokens so that the user does not need to reauthenticate each time a network connection is lost.	—	—
`CHAP`	Use CHAP with PPP authentication.	—	—
`EAP`	Use EAP-TLS with PPP authentication. Specify this protocol for Windows IPSec VPN clients that use Common Access Card (CAC) Smart Cards that contain user information and digital certificates.	—	—
`MSCHAP`	Use MSCHAP with PPP authentication.	—	—
`MSCHAPv2`	Use MSCHAPv2 with PPP authentication. This is the default for L2TP	—	—
`PAP`	Use PAP with PPP authentication.	—	—
`ppp securid`	If CACHE-SECURID is configured for PPP authentication, this specifies the time, in minutes, that the token is cached.	15-10080	1440 minutes

Usage Guidelines

L2TP/IPSec relies on the PPP connection process to perform user authentication and protocol configuration. You specify the protocol used for PPP authentication and whether SecureID tokens are cached on the WLAN switch. Client addresses are assigned from a pool configured with the **ip local pool** command.

Example

The following command configures virtual private dial-in networking:

```
vpdn group l2tp
  ppp authentication PAP
  client configuration dns 10.1.1.2
  client configuration wins 10.1.1.2
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server and/or Remote AP license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

vpdn group pptp

```
vpdn group pptp
  client configuration {dns|wins} <ipaddr1> [<ipaddr2>]
  disable|enable
  no ...
  ppp authentication {MSCHAP|MSCHAPv2}
  pptp echo <seconds>
```

Description

This command configures a PPTP VPN connection.

Syntax

Parameter	Description	Range	Default
`client configuration`	Configures parameters for the remote clients.	—	—
`dns`	Configures a primary and optional secondary DNS server.	—	—
`wins`	Configures a primary and optional secondary WINS server.	—	—
`disable|enable`	Disables or enables termination of PPTP clients.	—	enabled
`no`	Negates any configured parameter.	—	—
`ppp authentication`	Enables the protocols for PPP authentication. This list should match the PPTP configuration configured with the **vpn-dialer** command on the WLAN switch.	—	—
`MSCHAP`	Use MSCHAP with PPP authentication.	—	—
`MSCHAPv2`	Use MSCHAPv2 with PPP authentication. This is the default for L2TP	—	—
`pptp echo`	Time, in seconds, that the WLAN switch waits for a PPTP echo response from the client before considering the client to be down. The client is disconnected if it does not respond within this interval.	10-300	60 seconds

Usage Guidelines

PPTP connections require user-level authentication through a PPP authentication protocol (MSHCAPv2 is the currently-supported method.) Client addresses are assigned from a pool configured with the **pptp** command.

Example

The following command configures virtual private dial-in networking:

```
vpdn group pptp
  ppp authentication MSCHAPv2
  client configuration dns 10.1.1.2
  client configuration wins 10.1.1.2
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN server license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

vpn-dialer

```
vpn-dialer <name>
  enable dnetclear|l2tp|pptp|securid_newpinmode|wirednowifi
  ike {authentication {pre-share <key>|rsa-sig}|encryption {3des|des}|
   group {1|2}|hash {md5|sha}|lifetime [<seconds>]}
  ipsec {encryption {esp-3des|esp-des}|hash {esp-md5-hmac|esp-sha-hmac}|
   lifetime [<seconds>]|pfs {group1|group2}}
  no {enable...|ipsec...|ppp...}
  ppp authentication {cache-securid|chap|mschap|mschapv2|pap}
```

Description

This command configures the VPN dialer.

Syntax

Parameter	Description	Range	Default
<name>	Name that identifies this VPN dialer configuration.	—	—
enable	Enables dialer operations:	—	—
dnetclear	Enables “split tunneling” functionality so that traffic destined for the internal network is tunneled while traffic for the Internet is not. This option is not recommended for security reasons.	—	disabled
l2tp	Allows the dialer to negotiate a Layer-2 Tunneling Protocol (L2TP)/IPSec tunnel with the WLAN switch.	—	enabled
pptp	Allows the dialer to negotiate a Point-to-Point Tunneling Protocol (PPTP) with the WLAN switch.	—	disabled
securid_new pinmode	Supports SecurID new and next pin mode.	—	disabled
wirednowifi	Allows the dialer to detect when a wired network connection is in use, and shuts down the wireless interface.	—	disabled
ike	Configures internet key exchange (IKE) protocol. This configuration must match the IKE policy configured with the **crypto isakmp policy** command on the WLAN switch.	—	—
authentica tion	Specifies whether preshared keys or RSA signatures are used for IKE authentication.	pre-share | rsa-sig	pre-share
encryption	Specifies the IKE encryption protocol, either DES or 3DES.	3des | des	3des
group	Specifies the Diffie-Hellman group, either 1 or 2.	1 | 2	2
hash	Specifies the HASH algorithm, ether SHA or MD5.	md5 | sha	sha
lifetime	Specifies how long an IKE security association lasts, in seconds.	300-86400	28800 seconds
ipsec	Configures IPSec. This configuration must match the IPSec parameters configured with the **crypto dynamic-map** and **crypto ipsec** commands on the WLAN switch.	—	—
encryption	Specifies the encryption type for IPSec, either DES or 3DES.	esp-3des | esp-des	esp-3des
hash	Specifies the hash algorithm used by IPSec, either MD5 or SHA.	esp-md5-hmac | esp-sha- hmac	esp-sha-hmac

`lifetime`	Specifies how long an IPSec security association lasts, in seconds.	300-86400	7200 seconds
`pfs`	Specifies the IPSec Perfect Forward Secrecy (PFS) mode, either group 1 or group 2.	group1 | group2	group2
`no`	Negates any configured parameter.	—	—
`ppp authentication`	Enables the protocols for PPP authentication. This list should match the L2TP or PPTP configuration configured with the **vpdn** command on the WLAN switch.	—	—
`cache-securid`	The WLAN switch caches Secure ID tokens so that the user does not need to reauthenticate each time a network connection is lost.	—	disabled
`chap`	Use CHAP with PPP authentication.	—	enabled
`mschap`	Use MSCHAP with PPP authentication.	—	enabled
`mschapv2`	Use MSCHAPv2 with PPP authentication.	—	enabled
`pap`	Use PAP with PPP authentication.	—	enabled

Usage Guidelines

A VPN dialer is a Windows application that configures a Windows client for use with the VPN services in the WLAN switch. When VPN is used as an access method, a user can login using captive portal and download a VPN dialer. You can customize a VPN dialer for a user role configured with the **user-role** command. After the user authenticates via captive portal, a link appears to allow download of the VPN dialer if a dialer is configured for the user role.

Example

The following command configures a VPN dialer:

```
vpn-dialer default-dialer
  ike authentication pre-share f00xYz123BcA
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the VPN Server license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

vrrp

```
vrrp <id>
  advertise <interval>
  authentication <password>
  description <text>
  ip address <ipaddr>
  no...
  preempt
  priority <level>
  shutdown
  tracking interface {fastethernet <slot>/<port>|gigabitethernet <slot>/<port>}
 {sub <value>}
  tracking master-up-time <duration> add <value>
  tracking vlan <vlanid> {sub <value>}
  tracking vrrp-master-state <vrid> add <value>
  vlan <vlanid>
```

Description

This command configures the Virtual Router Redundancy Protocol (VRRP).

Syntax

Parameter	Description	Range	Default
id	Number that uniquely identifies the VRRP instance, also known as the VRID. This number should match the VRID on the other member of the redundant pair. For ease in administration, you should configure this with the same value as the VLAN ID. After you configure the VRID, the command platform enters VRRP mode. From here, you can access the remaining VRRP commands.	1-255	—
advertise	Specifies the time, in seconds, between successive VRRP advertisements sent by the current *master*. Alcatel-Lucent recommends that you use the default value.	1-60 seconds	1 second (1s=1000ms)
authentication	Configure an optional password of up to eight characters to be used to authenticate VRRP peers in their advertisements. The password must be the same on both members of the redundant pair. **NOTE:** The password is sent in plain-text and therefore should not be treated as a security measure. Rather, the purpose of the password is to guard against misconfigurations in the event that other VRRP devices exist on the same network.	8 characters	—
description	Configure an optional text string to describe the VRRP instance.	1-80 characters	—

`ip address`	Configure the virtual IP address that will be owned by the elected VRRP *master*. Use the same IP address on each member of the redundant pair. This IP address will be redundant - it will be active on the VRRP master, and will become active on the VRRP backup in the event that the VRRP master fails. The IP address must be unique; the IP address cannot be the loopback address of the WLAN switch. Only IPv4 address formats are supported.	—	—
`no`	Negates all configured VRRP parameters.	—	—
`preempt`	Preempt mode allows a WLAN switch to take over the role of master if it detects a lower priority WLAN switch currently acting as master. Alcatel-Lucent recommends that you use the default setting to avoid excessive interruption to users or "flapping" if a problematic WLAN switch is cycling up and down.	—	disabled
`priority`	Defines the priority level of the VRRP instance for the WLAN switch. This value is used in the election mechanism for the master. A higher number specifies a higher priority. The default priority setting is adequate for most networks.	100	1-255
`shutdown`	Administratively shutdown VRRP. When down, VRRP is not active, although the WLAN switch maintains the configuration information. To start the VRRP instance, use **no shutdown**.	—	enabled (VRRP is down)
`tracking interface`	Configures VRRP tracking based on Layer-2 interface state transitions. You can configure this on Fast Ethernet or Gigabit Ethernet interfaces. **NOTE:** You can track a combined maximum of 16 VLAN and Layer-2 interfaces.	—	—
`<slot>`	<slot> is always 1 except for the OAW-6000 WLAN switch, where the slots can be 0, 1, 2, or 3.	—	—
`<port>`	Number assigned to the network interface embedded in the WLAN switch or in the line card installed in the OAW-6000 WLAN switch. Port numbers start at 0 from the left-most position.	—	—
`sub`	Decreases the priority of the VRRP instance by the specified amount. When the interface comes up again, the value is restored to the previous priority level. **NOTE:** The combined priority and tracking vales cannot exceed 255. If the priority value exceeds 255, the WLAN switch displays an error message.	0-255	—
`tracking master-up-time duration`	Monitors how long the WLAN switch has been master for the VRRP instance.	0-1440 minutes	—

`tracking master-up-time add`	Instructs the WLAN switch to add the specified value to the existing priority level. **NOTE:** The combined priority and tracking values cannot exceed 255. If the priority value exceeds 255, the WLAN switch displays an error message similar to the following: `Error: Vrrp 30 priority + tracking value exceeds 255`	0-255	—
`tracking vlan`	Configures VRRP tracking based on VLAN state transitions. **NOTE:** You can track a combined maximum of 16 VLAN and Layer-2 interfaces.	—	—
`sub`	Decreases the priority of the VRRP instance by the specified amount. When the VLAN comes up again, the value is restored to the previous priority level. **NOTE:** The combined priority and tracking values cannot exceed 255. If the priority value exceeds 255, the WLAN switch displays an error message.	0-255	—
`vrrp-master-state`	Specifies the VRID to use for tracking the state of the VRRP master WLAN switch.	1-255	—
`vrrp-master-state add`	Instructs the WLAN switch to add the specified value to the existing priority level. **NOTE:** The combined priority and tracking values cannot exceed 255. If the priority value exceeds 255, the WLAN switch displays an error message similar to the following: `Error: Vrrp 30 priority + tracking value exceeds 255`	0-255	—
`vlan`	Specifies the VLAN ID of the VLAN on which VRRP will run.	1-4094	—

Usage Guidelines

Use this command to set parameters for VRRP on the WLAN switch. The default VRRP parameters can be left for most implementations.

You can use a combination of numbers, letters, and characters to create the authentication password and the VRRP description. To include a space in the password or description, enter quotation marks around the string. For example, to create the password Floor 1, enter “Floor 1” at the prompt.

To change the existing password or description, enter the command with a different string. The new password or description takes affect immediately.

To unconfigure the existing password or description, enter “” at the prompt.

NOTE: If you update the password on one WLAN switch, you must update the password on the redundant member pair.

Interface Tracking

You can track multiple VRRP instances to prevent asymmetric routing and dynamically change the VRRP master to adapt to changes in the network. VRRP interface tracking can alter the priority of the VRRP instance based on the state of a particular VLAN or Layer-2 interface. The priority of the VRRP instance can increase or decrease based on the operational state of the specified interface.

For example, interface transitions (up/down events) can trigger a recomputation of the VRRP priority, which can change the VRRP master depending on the resulting priority. You can track a combined maximum of 16 interfaces.

NOTE: You must enable preempt mode to allow a WLAN switch to take over the role of master if it detects a lower priority WLAN switch currently acting as master.

Example

The following command configures a priority of 105 for VRRP ID (VRID) 30:

```
vrrp 30
  priority 105
```

The following commands configure VLAN interface tracking and assumes the following:

- You have two WLAN switches, a primary and a backup.
- The configuration highlights the parameters for interface tracking. You may have other parameters configured for VRRP.

Primary Configuration

```
vrrp 10
  vlan 10
  ip address 10.200.22.254
  priority 105
  preempt
  tracking vlan 20 sub 10

vrrp 20
  vlan 20
  ip address 10.200.22.254
  preempt
  priority 105
  tracking vlan 10 sub 10

vrrp 30
  vlan 30
  ip address 10.200.22.254
  preempt
  priority 105
  tracking vlan 20 sub 10
```

Backup Configuration

```
vrrp 10
  vlan 10
  ip address 10.200.22.254
  priority 100
  preempt
  tracking vlan 20 sub 10

vrrp 20
  vlan 20
  ip address 10.200.22.254
  preempt
  priority 100
  tracking vlan 10 sub 10

vrrp 30
  vlan 30
  ip address 10.200.22.254
  preempt
  priority 100
  tracking vlan 20 sub 10
```

If VLAN 20 goes down, VRRP 20 automatically fails over, VRRP 10 and VRRP 30 would drop their priority to 95, causing a failover to the backup WLAN switch. Once VLAN 20 comes back up, the primary WLAN switch restores the VRRP priority to 105 for all VRRP IDs and resumes the master VRRP role.

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 1.0.

The tracking interface and tracking vlan parameters were introduced in AOS-W 3.3.

The add option was deprecated from the tracking interface and tracking vlan parameters in AOS-W 3.3.2.

web-server

```
web-server
   captive-portal-cert <name>
   ciphers {high|low|medium}
   mgmt-auth [certificate] [username/password]
   no ...
   ssl-protocol [sslv2] [sslv3] [tlsvl]
   switch-cert <name>
```

Description

This command configures the WLAN switch's web server.

Syntax

Parameter	Description	Range	Default
`captive-portal-cert`	Name of the server certificate associated with captive portal. Use the **show crypto-local pki ServerCert** command to see the server certificates installed in the WLAN switch.	—	default
`ciphers`	Configures the strength of the cipher suite: high: encryption keys larger than 128 bits low: 56 or 64 bit encryption keys medium: 128 bit encryption keys	high, low, medium	high
`mgmt-auth`	Authentication method for the management user; you can choose to use either username/password or certificates, or both username/password and certificates.	username/ password, certificate	username/ password
`no`	Negates any configured parameter.	—	—
`ssl-protocol`	Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol version used for securing communication with the web server: SSLv3 TLSv1	sslv3, tlsv1	sslv3, tlsv1
`switch-cert`	Name of the server certificate associated with WebUI access. Use the **show crypto-local pki ServerCert** command to see the server certificates installed in the WLAN switch.	—	default

Usage Guidelines

There is a default server certificate installed in the WLAN switch, however this certificate does not guarantee security in production networks. Alcatel-Lucent strongly recommends that you replace the default certificate with a custom certificate issued for your site by a trusted Certificate Authority (CA). See the *AOS-W User Guide* for more information about how to generate a Certificate Signing Request (CSR) to submit to a CA and how to import the signed certificate received from the CA into the WLAN switch. After importing the signed certificate into the WLAN switch, use the **web-server** command to specify the certificate for captive portal or WebUI access. If you need to specify a different certificate for captive portal or WebUI access, use the **no** command to revert back to the default certificate before you specify the new certificate (see the Example section).

You can use client certificates to authenticate management users. If you specify certificate authentication, you need to configure certificate authentication for the management user with the **mgmt-user webui-cacert** command.

Example

The following commands configure WebUI access with client certificates only, and specify the server certificate for the WLAN switch:

```
web-server mgmt-auth certificate
   switch-cert ServerCert1

mgmt-user webui-cacert serial 1111111 web-admin root
```

To specify a different server certificate, use the **no** command to revert back to the default certificate *before* you specify the new certificate:

```
web-server mgmt-auth certificate
   switch-cert ServerCert1
   no switch-cert
   switch-cert ServerCert2
```

Platform Availability

This command is available on all platforms. The **web-server ciphers** and **web-server ssl-protocol** commands require the PEF license.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

The mgmt-auth parameter was introduced in AOS-W 3.1.

The captive-portal-cert parameter was introduced in AOS-W 3.2.

whoami

```
whoami
```

Description

This command displays information about the current user logged into the WLAN switch.

Syntax

No parameters.

Usage Guidelines

Use this command to display the name and role of the user who is logged into the WLAN switch for this session.

Example

The following command displays information about the user logged into the WLAN switch:

```
whoami
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable and config modes on master WLAN switches.

History

This command was available in AOS-W 1.0.

wlan edca-parameters-profile

```
wlan edca-parameters-profile {ap|station} <profile>
  {background | best-effort | video | voice}
  [acm][aifsn <number>] [ecw-max <exponent> [ecw-min <exponent>] [txop <number>]
  [clone <profile>
```

Description

This command configures an enhanced distributed channel access (EDCA) profile for APs or for clients (stations).

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`background`	Configures the background queue.	—	—
`best-effort`	Configures the best-effort queue.	—	—
`video`	Configures the video queue.	—	—
`voice`	Configures the voice queue.	—	—
`acm`	Specifies mandatory admission control. The client reserves the access category through traffic specification (TSPEC) signaling. Enter 1 to enable, 0 to disable.	0, 1	0 (disabled)
`aifsn`	Arbitrary inter-frame space number.	1-15	0
`ecw-max`	The exponential (n) value of the maximum contention window size, as expressed by 2^n-1. A value of 4 computes to 2^4-1 = 15.	1-15	0
`ecw-min`	The exponential (n) value of the minimum contention window size, as expressed by 2^n-1. A value of 4 computes to 2^4-1 = 15.	0-15	0
`txop`	Transmission opportunity, in units of 32 microseconds. Divide the desired transmission duration by 32 to determine the value to configure. For example, for a transmission duration of 3008 microseconds, enter 94 (3008/32).	0-2047	0
`clone`	Name of an existing EDCA profile from which parameter values are copied.	—	—

Usage Guidelines

NOTE: Use this command only under the guidance of your Alcatel-Lucent representative.

EDCA profiles are specific either to APs or clients. You apply an EDCA profile to a specific SSID profile.

The following are the default values configured for APs:

Access Category	ecw-min	ecw-max	aifsn	txop	acm
best-effort	4	6	3	0	No
background	4	10	7	0	No
video	3	4	1	94	No
voice	2	3	1	47	No

The following are the default values configured for clients:

Access Category	ecw-min	ecw-max	aifsn	txop	acm
best-effort	4	10	3	0	No
background	4	10	7	0	No
video	3	4	2	94	No
voice	2	3	2	47	No

Example

The following command configures an EDCA profile for APs:

```
wlan edca-parameters-profile ap edca1
   best-effort ecw-min 15 ecw-max 15 aifsn 15 txop 100 acm 1
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Voice Services Module license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.1.

wlan ht-ssid-profile

```
wlan ht-ssid-profile <profile>
  40MHz-enable
  allow-weak-encryption
  clone <profile>
  high-throughput-enable
  legacy-stations
  max-rx-a-mpdu-size {8191|16383|32767|65535}
  max-tx-a-mpdu-size <bytes>
  min-mpdu-start-spacing {0|.25|.5|1|2|4|8|16}
  mpdu-agg
  no...
  short-guard-intvl-40MHz
  supported-mcs-set <mcs-list>
```

Description

This command configures a high-throughput SSID profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`40MHz-enable`	Enables or disables the use of this high-throughput SSID in 40 MHz mode.	—	enabled
`allow-weak-encryption`	The use of TKIP or WEP for unicast traffic forces the use of legacy transmissions rates. Disabling this mode prevents the association of stations using TKIP or WEP for unicast traffic. This mode is disabled by default.	—	disabled
`clone`	Name of an existing high-throughput SSID profile from which parameter values are copied.	—	—
`high-throughput-enable`	Determines if this high-throughput SSID allows high-throughput (802.11n) stations to associate. **NOTE:** Enabling high-throughput in an ht-ssid-profile enables Wi-Fi Multimedia (WMM) base features for the associated SSID.	—	enabled
`legacy-stations`	Controls whether or not legacy (non-HT) stations are allowed to associate with this SSID. By default, legacy stations are allowed to associate. **NOTE:** This setting has no effect on a BSS in which HT support is not available.	—	enabled
`max-rx-a-mpdu-size`	Controls the maximum size, in bytes, of an Aggregated-MAC Packet Data Unit (A-MPDU) that can be received on this high-throughput SSID.	8191/16383/ 32767/65535	65535
`8191`	Maximum size of 8191 bytes.		
`16383`	Maximum size of 16383 bytes.		
`32767`	Maximum size of 32767 bytes.		
`65535`	Maximum size of 65535 bytes.		
`max-tx-a-mpdu-size`	Controls the maximum size, in bytes, of an A-MPDU that can be sent on this high-throughput SSID.	1576-65535	65535
`min-mpdu-start-spacing`	Minimum time between the start of adjacent MDPUs within an aggregate MDPU in microseconds.	0/.25/.5/1/2/ 4/8/16	0

0	No restriction on MDPU start spacing.		
.25	Minimum time of .25 µsec.		
.5	Minimum time of .5 µsec.		
1	Minimum time of 1 µsec.		
2	Minimum time of 2 µsec.		
4	Minimum time of 4 µsec.		
8	Minimum time of 8 µsec.		
16	Minimum time of 16 µsec.		
mpdu-agg	Enables or disables MAC protocol data unit (MDPU) aggregation.	—	enabled
no	Negates any configured parameter.	—	—
short-guard-intvl-40MHz	Enables or disables use of short guard interval in 40 MHz mode of operation.		enabled
supported-mcs-set	Comma-separated list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this high-throughput SSID.	0-15	0-15

Usage Guidelines

The ht-ssid-profile configures the high-throughput SSID.

NOTE: AP configuration settings related to the IEEE 802.11n draft standard are configurable for Alcatel-Lucent's OAW-AP120 series access points, which are IEEE 802.11n draft standard compliant devices.

De-aggregation of MAC Service Data Units (A-MSDUs) is supported on the OmniAccess 4504, 4604, and 4704 WLAN switches and the OmniAccess Supervisor Card III (OAW-S3) with a maximum frame transmission size of 4k bytes; however, this feature is always enabled and is not configurable. Aggregation is not currently supported.

Example

The following command configures the maximum size of a received aggregate MDPU to be 8191 bytes for the high-throughput SSID named "htcorpnet:"

```
wlan ht-ssid-profile htcorpnet
  max-rx-a-mpdu-size 8191
```

Platform Availability

This command is available on all platforms but operates with IEEE 802.11n compliant devices only.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was introduced in AOS-W 3.3. The legacy-stations parameter was introduced in AOS-W 3.3.1.

De-aggregation of MAC Service Data Units (A-MSDUs) on the OmniAccess 4504, 4604, and 4704 WLAN switches and the OmniAccess Supervisor Card III (OAW-S3) was introduced in AOS-W 3.3.2.

wlan ssid-profile

```
wlan ssid-profile <profile>
  902il-compatibility-mode
  a-basic-rates <mbps>
  a-tx-rates <mbps>
  ageout <seconds>
  battery-boost
  clone <profile>
  deny-bcast
  dtim-period <milliseconds>
  edca-parameters-profile {ap|station} <profile>
  essid <name>
  g-basic-rates <mbps>
  g-tx-rates <mbps>
  hide-ssid
  ht-ssid-profile <profile>
  local-probe-response
  max-clients <number>
  max-retries <number>
  max-tx-fail <number>
  mcast-rate-opt
  no ...
  opmode {dynamic-wep opensystem static-wep wpa-aes wpa-psk-aes wpa-psk-tkip wpa-tkip
   wpa2-aes wpa2-psk-aes wpa2-psk-tkip wpa2-tkip xSec}
  rts-threshold <number>
  short-preamble
  ssid-enable
  wepkey1 <key> [wepkey2 <key>] [wepkey3 <key>] [wepkey4 <key>]
  weptxkey <index>
  wmm
  wmm-be-dscp <best-effort>
  wmm-bk-dscp <background>
  wmm-ts-min-inact-int <milliseconds>
  wmm-vi-dscp <video>
  wmm-vo-dscp <voice>
  wpa-hexkey <psk>
  wpa-passphrase <string>
```

Description

This command configures an SSID profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`902il-compatibility-mode`	(For clients using NTT DoCoMo 902iL phones only) When enabled, the WLAN switch does not drop packets from the client if a small or old initialization vector value is received. (When TKIP or AES is used for encryption and TSPEC is enabled, the phone resets the value of the initialization vector after add/delete TSPEC.) **NOTE**: The Voice Services Module license must be installed.	—	disabled
`a-basic-rates`	List of supported 802.11a rates, in Mbps, that are advertised in beacon frames and probe responses.	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 12, 24 Mbps

a-tx-rates	Set of 802.11a rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error/loss rate of the client.	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps
ageout	Time, in seconds, that a client is allowed to remain idle before being aged out.		1000 seconds
battery-boost	Converts multicast traffic to unicast before delivery to the client, thus allowing you to set a longer DTIM interval. The longer interval keeps associated wireless clients from activating their radios for multicast indication and delivery, leaving them in power-save mode longer and thus lengthening battery life. **NOTE:** The Voice Services Module license must be installed.	—	disabled
clone	Name of an existing SSID profile from which parameter values are copied.	—	—
deny-bcast	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.	—	disabled
dtim-period	Specifies the interval, in milliseconds, between the sending of Delivery Traffic Indication Messages (DTIMs) in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed. When using wireless clients that employ power management features to sleep, the client must revive at least once during the DTIM period to receive broadcasts.		1
edca-parameters-profile	Name of the enhanced distributed channel access (EDCA) profile that applies to this SSID. **NOTE:** This profile requires the Voice Services Module license in the WLAN switch. Configure this parameter only under the guidance of your Alcatel-Lucent representative.	—	—
ap|sta	Assigns the specified EDCA profile to AP or station (client).	—	—
essid	Name that uniquely identifies the Service Set Identifier (SSID). The SSID can be up to 31 characters.	—	“alcatel-ap”
g-basic-rates	List of supported 802.11b/g rates that are advertised in beacon frames and probe responses.	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2 Mbps
g-tx-rates	Set of 802.11b/g rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error/loss rate of the client.	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
hide-ssid	Enables or disables hiding of the SSID name in beacon frames. Note that hiding the SSID does very little to increase security.	—	disabled
ht-ssid-profile	Name of high-throughput SSID profile to use for configuring high-throughput support. See “wlan ht-ssid-profile” on page 378.	—	“default”

local-probe-response	Enable or disable local probe response on the AP. If this option is enabled, the AP is responsible for sending 802.11 probe responses to wireless clients' probe requests. If this option is disabled, then the WLAN switch sends the 802.11 probe responses.	—	enabled
max-clients	Maximum number of wireless clients for the AP.	0-256	64
max-retries	Maximum number of retries allowed for the AP to send a frame.	0-15	4
max-tx-fail	Maximum transmission failures allowed before the client gives up.		0
mcast-rate-opt	Enables or disables scanning of all active stations currently associated to an AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate. **NOTE:** Do not enable this parameter unless instructed to do so by your Alcatel-Lucent representative.	—	disabled
no	Negates any configured parameter.	—	—
opmode	The layer-2 authentication and encryption to be used on this ESSID to protect access and ensure the privacy of the data transmitted to and from the network.	(see following)	opensystem
dynamic-wep	WEP with dynamic keys.		
opensystem	No authentication and encryption.		
static-wep	WEP with static keys.		
wpa-aes	WPA with AES encryption and dynamic keys using 802.1x.		
wpa-psk-aes	WPA with AES encryption using a preshared key.		
wpa-psk-tkip	WPA with TKIP encryption using a preshared key.		
wpa-tkip	WPA with TKIP encryption and dynamic keys using 802.1x.		
wpa2-aes	WPA2 with AES encryption and dynamic keys using 802.1x.		
wpa2-psk-aes	WPA2 with AES encryption using a preshared key.		
wpa2-psk-tkip	WPA2 with TKIP encryption using a preshared key.		
wpa2-tkip	WPA2 with TKIP encryption and dynamic keys using 802.1x.		
xSec	Encryption and tunneling of Layer-2 traffic between the WLAN switch and wired or wireless clients, or between WLAN switches. To use xSec encryption, you must use a RADIUS authentication server. For clients, you must install the Funk Odyssey client software. **NOTE:** Requires installation of the xSec license. For xSec between WLAN switches, you must install an xSec license in each WLAN switch.		
rts-threshold	Wireless clients transmitting frames larger than this threshold must issue Request to Send (RTS) and wait for the AP to respond with Clear to Send (CTS). This helps prevent mid-air collisions for wireless clients that are not within wireless peer range and cannot detect when other wireless clients are transmitting.		2333 bytes

short-preamble	Enables or disables short preamble for 802.11b/g radios. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using short preamble. To use only long preamble, disable short preamble. Legacy client devices that use only long preamble generally can be updated to support short preamble.	—	enabled
ssid-enable	Enables/disables this SSID.	—	enabled
wepkey1 - wepkey4	Static WEP key associated with the key index. Can be 10 or 26 hex characters in length.	—	—
weptxkey	Key index that specifies which static WEP key is to be used. Can be 1, 2, 3, or 4.	1, 2, 3, 4	1
wmm	Enables or disables WMM, also known as IEEE 802.11e Enhanced Distribution Coordination Function (EDCF). WMM provides prioritization of specific traffic relative to other traffic in the network.	—	disabled
wmm-be-dscp	DSCP used to map WMM voice traffic.	0-255	24
wmm-bk-dscp	DSCP used to map WMM background traffic.	0-255	8
wmm-ts-min-in act-int	Specifies the minimum inactivity time-out threshold of WMM traffic. This setting is useful in environments where low inactivity interval time-outs are advertised, which may cause unwanted timeouts.	0-3,600,000	0 milliseconds
wmm-vi-dscp	DSCP used to map WMM video traffic.	0-255	40
wmm-vo-dscp	DSCP used to map WMM voice traffic.	0-255	56
wpa-hexkey	WPA pre-shared key (PSK).	—	—
wpa-passphrase	WPA passphrase with which to generate a pre-shared key (PSK).	—	—

Usage Guidelines

The SSID profile configures the SSID.

NOTE: AP configuration settings related to the IEEE 802.11n draft standard are configurable for Alcatel-Lucent's OAW-AP120 series access points, which are IEEE 802.11n draft standard compliant devices.

Default WMM mappings exist for all SSIDs. After you customize an WMM mapping and apply it to the SSID, the WLAN switch overwrites the default mapping values and uses the user-configured values.

Example

The following command configures an SSID for WPA2 AES authentication:

```
wlan ssid-profile corpnet
   ssid Corpnet
   opmode wpa2-aes
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for the noted parameters.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

The wmm-ts-min-inact-int parameter was introduced in AOS-W 3.2. The wpa2-preauth parameter was removed in AOS-W 3.2.

Support for the high-throughput IEEE 802.11n draft standard was introduced in AOS-W 3.3, including the ht-ssid-profile parameter and various rate changes.

Support for configurable WMM AC mapping was introduced in AOS-W 3.3.1, including the wmm-be-dscp, wmm-bk-dscp, wmm-vi-dscp, and wmm-vo-dscp parameters.

wlan traffic-management-profile

```
wlan traffic-management-profile <profile>
  bw-alloc virtual-ap <virtual-ap> share <percent>
  clone <profile>
  no ...
  report-interval <minutes>
```

Description

This command configures a traffic management profile.

Syntax

Parameter	Description	Range	Default
<profile>	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
bw-alloc	Minimum bandwidth, as a percentage of available bandwidth, allocated to an SSID when there is congestion on the wireless network. An SSID can utilize all available bandwidth if no other SSIDs are active.		
virtual-ap	Name of the virtual AP profile which pertains to the SSID.	—	—
share	Percentage of available bandwidth allocated to this SSID.	0-100	—
clone	Name of an existing traffic management profile from which parameter values are copied.	—	—
no	Negates any configured parameter.	—	—
report-interval	Number of minutes between bandwidth usage reports.		5 minutes

Usage Guidelines

The traffic management profile allows you to allocate bandwidth to SSIDs.

Example

The following command configures a traffic management profile that allocates bandwidth to the corpnet virtual AP:

```
wlan traffic-management-profile best
  bw-alloc virtual-ap corpnet share 75
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system on master WLAN switches.

Command Mode

This command is available in config mode.

History

This command was available in AOS-W 3.0.

The mode parameters were introduced in AOS-W 3.2.

wlan virtual-ap

```
wlan virtual-ap <profile>
  aaa-profile <profile>
  allowed-band <band>...
  auth-failure-blacklist-time <seconds>
  band-steering (not intended for use)
  blacklist
  blacklist-time <seconds>
  clone <profile>
  dos-prevention
  deny-time-range <range>
  fast-roaming
  forward-mode {bridge|split-tunnel|tunnel}
  ha-disc-onassoc
  mobile-ip
  no ...
  rap-operation {always|backup|persistent|standard}
  ssid-profile <profile>
  strict-compliance
  vap-enable
  vlan <vlan>...
  vlan-mobility
  voip-proxy-arp
```

Description

This command configures a virtual AP profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`aaa-profile`	Name of the AAA profile that applies to this virtual AP.	—	"default"
`allowed-band`	The band(s) on which to use the virtual AP: ■ a—802.11a band only (5 GHz) ■ g—802.11b/g band only (2.4 GHz) ■ all—both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz)	a/g/all	all
`auth-failure-blacklist-time`	Time, in seconds, a client is blocked if it fails repeated authentication. 0 blocks indefinitely.		0
`band-steering`	This parameter is intended for use in a lab environment only and is not a released feature. Do not use this parameter without proper guidance from Alcatel-Lucent.	Not intended for use.	Not intended for use.
`blacklist`	Enables detection of denial of service (DoS) attacks, such as ping or SYN floods, that are not spoofed deauth attacks.	—	enabled
`blacklist-time`	Number of seconds that a client is quarantined from the network after being blacklisted.		3600 seconds (1 hour)
`clone`	Name of an existing traffic management profile from which parameter values are copied.	—	—
`deny-time-range`	Time range for which the AP will deny access.	—	—

dos-prevention	If enabled, APs ignore deauthentication frames from clients. This prevents a successful deauth attack from being carried out against the AP. This does not affect third-party APs.	—	disabled
fast-roaming	Enable or disable fast roaming.	—	disabled
forward-mode	Controls whether 802.11 frames are tunneled to the WLAN switch using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the WLAN switch, and Internet access remains local). Only 802.1x authentication is supported when configuring bridge or split tunnel mode. **NOTE:** For split tunnel mode, the Remote AP license must be installed.	bridge/split-tunnel/tunnel	tunnel
ha-disc-onassoc	If enabled, all clients of a virtual-ap will received mobility service on association.	—	disabled
mobile-ip	Enables or disables IP mobility for this virtual AP.	—	enabled
no	Negates any configured parameter.	—	—
rap-operation	Configures when the virtual AP operates on a remote AP: ■ always—Permanently enables the virtual AP ■ backup—Enables the virtual AP if the remote AP cannot connect to the WLAN switch ■ persistent—Permanently enables the virtual AP after the remote AP initially connects to the WLAN switch ■ standard—Enables the virtual AP when the remote AP connects to the WLAN switch Use always and backup for bridge SSIDs. Use persistent and standard for 802.1x, tunneled, and split-tunneled SSIDs. **NOTE:** The Remote AP license must be installed.	always/ backup/ persistent/ standard	standard
ssid-profile	Name of the SSID profile that applies to this virtual AP.	—	"default"
strict-compliance	If enabled, the AP denies client association requests if the AP and client station have no common rates defined. Some legacy client stations which are not fully 802.11-compliant may not include their configured rates in their association requests. Such non-compliant stations may have difficulty associating with APs unless strict compliance is disabled.	—	disabled
vap-enable	Enable or disable the virtual AP.	—	enabled
vlan	The VLAN(s) into which users are placed in order to obtain an IP address.	—	1
vlan-mobility	Enable or disable VLAN (Layer-2) mobility.	—	disabled
voip-proxy-arp	If enabled, all broadcast ARP requests are converted to unicast and sent directly to the client. You can check the status of this option using the `show ap active` and the `show datapath tunnel` command. If enabled, the output will display the alphabet **a** in the flags column. **NOTE:** Voice license must be installed.	—	disabled

Usage Guidelines

Wireless LAN profiles configure WLANs in the form of virtual AP profiles. A virtual AP profile contains an SSID profile which defines the WLAN and an AAA profile which defines the authentication for the WLAN. You can configure and apply multiple instances of virtual AP profiles to an AP group or to an individual AP.

Example

The following command configures a virtual AP:

```
wlan virtual-ap corpnet
   vlan 1
   aaa-profile corpnet
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system, except for the noted parameters.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

Support for the split tunneling option and the rap-operation parameter was introduced in AOS-W 3.2.

In support of the IEEE 802.11n draft standard, a change to the allowed-band parameter was introduced in AOS-W 3.3.

Support for the ha-disc-onassoc parameter was introduced in AOS-W 3.3.2.

The band-steering parameter is not a released feature and was introduced in AOS-W 3.3.2 for intended use in a lab environment only. Do not use band-steering without proper guidance from Alcatel-Lucent.

Support for the voip-proxy-arp parameter was introduced in AOS-W 3.3.2.

wlan voip-cac-profile

```
wlan voip-cac-profile <profile>
  active-load-balancing
  call-admission-control
  call-handoff-reservation <percent>
  clone <profile>
  disconnect-extra-call
  drop-sip-invite-for-cac
  high-capacity-threshold <percent>
  no ...
  noe-call-capacity <number>
  sccp-call-capacity <number>
  send-sip-100-trying
  sip-call-capacity <number>
  svp-call-capacity <number>
  vocera-call-capacity <number>
  wmm_tspec_enforcement
  wmm_tspec_enforcement_period <seconds>
```

Description

This command configures a voice over iP (VoIP) call admission control (CAC) profile.

Syntax

Parameter	Description	Range	Default
<profile>	Name of this instance of the profile. The name must be 1-63 characters.	—	“default”
active-load-balancing	If enabled, idle VoIP clients are kicked off the radio when VoIP capacity thresholds are reached.	—	disabled
call-admission-control	Enables or disable VoIP CAC features.	—	disabled
call-handoff-reservation	Percentage of call capacity reserved for mobile VoIP clients on call.	0-100	20%
clone	Name of an existing VoIP CAC profile from which parameter values are copied.	—	—
disconnect-extra-call	Disconnects calls that exceed the high capacity threshold by sending a deauthentication frame.	—	disabled
high-capacity-threshold	Percentage of remaining call capacity that enables load balancing for all new clients.	0-100	20%
no	Negates any configured parameter.	—	—
noe-call-capacity	Number of simultaneous NOE calls that can be handled by one radio.	—	10
sccp-call-capacity	Number of simultaneous Cisco SCCP calls that can be handled by one radio.	—	10
send-sip-100-trying	Enables sending of SIP 100 - trying messages to a call originator to indicate that the call is proceeding. This is useful when the SIP invite may be redirected through a number of servers before reaching the WLAN switch.	—	enabled
sip-call-capacity	Number of simultaneous SIP calls that can be handled by one radio.	—	10
svp-call-capacity	Number of simultaneous SVP calls that can be handled by one radio.	—	10

vocera-call-capacity	Number of simultaneous Vocera calls that can be handled by one radio.	—	10
wmm_tspec_enforcement	Enables validation of TSPEC requests for CAC.	—	disabled
wmm_tspec_enforcement_period	Maximum time for the station to start the call after the TSPEC request.	1-100	1 second

Usage Guidelines

The VoIP CAC profile prevents any single AP from becoming congested with voice calls.

Example

The following command enables VoIP CAC:

```
wlan voip-cac-profile cac1
   call-admission-control
   disconnect-extra-call
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command requires the Voice Services Module license.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

wms ap

```
wms ap <bssid> mode
{dos|interfering|known-interfering|suspect-unsecure|unsecure|valid}
```

Description

This command allows you to classify an AP into one of several categories.

Syntax

Parameter	Description	Range	Default
ap	BSSID of the AP	—	—
mode	Classify the AP into one of the following categories:	—	—
dos	Enables denial of service for this AP. Any clients connected to this AP are disconnected.		
interfering	An AP seen in the RF environment but is not connected to the wired network.		
known-interfering	An interfering AP whose BSSID is known.		
suspect-unsecure	A suspected rogue AP that is plugged into the wired side of the network but may not be an unauthorized device. Automatic shutdown of rogue APs does not apply to these devices.		
unsecure	A rogue AP that is unauthorized and is plugged into the wired side of the network. You can configure automatic shutdown of rogue APs in the IDS unauthorized device detection profile.		
valid	An AP that is part of the enterprise providing WLAN service.		

Usage Guidelines

If AP learning is enabled (with the wms general learn-ap enable command), non-OmniAccess APs connected on the same wired network as OmniAccess APs are classified as valid APs. If AP learning is disabled, a non-OmniAccess AP is classified as an unsecure or suspect-unsecure AP.

Example

The following command classifies an interfering AP as a known-interfering AP:

```
wms ap 01:00:00:00:00:00 mode known-interfering
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

wms clean-db

```
wms clean-db
```

Description

This command deletes the WMS database.

Syntax

Parameter	Description	Range	Default
`clean-db`	Cleans the WMS database.	—	—

Usage Guidelines

This command deletes all entries from the WMS database. Do not use this command unless instructed to do so by an Alcatel-Lucent representative.

Example

The following command cleans the WMS database:

```
wms clean-db
WMS Database will be deleted. Do you want to proceed with this action [y/n]:
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

wms client

```
wms client <macaddr> mode {dos|interfering|valid}
```

Description

This command allows you to classify a wireless client into one of several categories.

Syntax

Parameter	Description	Range	Default
`client`	MAC address of the client.	—	—
`mode`	Classify the client into one of the following categories:	—	—
`dos`	Enables denial of service to this client.		
`interfering`	A client seen in the RF environment that is outside of the enterprise.		
`valid`	A client that is part of the enterprise.		

Usage Guidelines

AOS-W can automatically determine client classification based on client behavior, but this command allows you to explicitly classify a client. The classification of a client is used in certain policy enforcement features. For example, if protect-valid-sta is enabled in the IDS Unauthorized Device Profile, then clients that are classified as valid cannot connect to non-valid APs.

Example

The following command classifies a client as valid:

```
wms client 00:00:A4:34:C9:B3 mode valid
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

wms export-class

```
wms export-class <filename>
```

Description

This command exports classification information into a file.

Syntax

Parameter	Description	Range	Default
`export-class`	Filename	—	—

Usage Guidelines

This command writes classification data into comma separated values (CSV) files—one for APs and one for clients. You can import these files into the OmniVista Mobility Manager.

Example

The following command exports classification data into an AP and a client file:

```
wms export-class class

Exported data to class_ap.csv and class_sta.csv
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

wms export-db

```
wms export-db <filename>
```

Description

This command exports the WMS database to a specified file.

Syntax

Parameter	Description	Range	Default
`export-db`	Filename. The filename plus any extensions must be no longer than 32 characters and may contain only keyboard characters.	—	—

Usage Guidelines

The file is exported as an ASCII text file.

NOTE: If you have configured the WLAN switch for operation with the OmniVista Mobility Manager (OV-MM), this command will fail and an error will be returned.

Example

The following command exports the WMS database to a file:

```
wms export-db database
```

```
Exported WMS DB to database
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

wms general

```
wms general ap-ageout-interval <minutes> | collect-stats {disable|enable} |
learn-ap {enable|disable} | persistent-known-interfering {enable|disable} |
poll-interval <milliseconds> |poll-retries <number> | propagate-wired-macs
{enable|disable} | sta-ageout-interval <minutes> | stat-update {enable|disable}
```

Description

This command configures the WLAN management system (WMS).

Syntax

Parameter	Description	Range	Default
`ap-ageout-interval`	Time, in minutes, that an AP remains unseen by any probes before it is deleted from the database.	0 to disable	30 minutes
`collect-stats`	Enables collection of statistics (up to 25,000 entries) on the master WLAN switch for monitored APs and clients. This only applies when OV-MM is not configured.	enable| disable	disabled
`learn-ap`	Enables “learning” of non-OmniAccess APs.	enable| disable	disabled
`persistent-known-interfering`	Enables APs that are marked as known interfering from being aged out.	enable| disable	disabled
`poll-interval`	Interval, in milliseconds, for communication between the WLAN switch and OmniAccess AMs. The WLAN switch contacts the AM at this interval to download AP to station associations, update policy configuration changes, and download AP and station statistics.	(any)	60000 milliseconds (1 minute)
`poll-retries`	Maximum number of failed polling attempts before the polled AM is considered to be down.	(any)	2
`propagate-wired-macs`	Enables the propagation of the gateway wired MAC information.	enable| disable	enabled
`sta-ageout-interval`	Time, in minutes, that a client remains unseen by any probes before it is deleted from the database.	0 to disable	30 minutes
`stat-update`	Enables statistics updating in the database.	enable| disable	enabled

Usage Guidelines

By default, non-OmniAccess APs that are connected on the same wired networks as OmniAccess APs are classified as “rogue” APs. Enabling AP learning classifies non-OmniAccess APs as “valid” APs. Typically, you would want to enable AP learning in environments with large numbers of existing non-OmniAccess APs and leave AP learning enabled until all APs in the network have been detected and classified as valid. Then, disable AP learning and reclassify any unknown APs as interfering.

Example

The following command enables AP learning:

```
wms general learn-ap enable
```

To disable AP learning:

```
wms general learn-ap disable
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in config mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

wms import-db

```
wms import-db <filename>
```

Description

This command imports the specified file into the WMS database.

Syntax

Parameter	Description	Range	Default
`import-db`	Filename	—	—

Usage Guidelines

The imported file replaces the WMS database. The imported file must be a valid WMS database file that you previously exported using the **wms export-db** command.

Example

The following command imports the WMS database from a file:

```
wms import-db database
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

wms reinit-db

```
wms reinit-db
```

Description

This command reinitializes the WMS database to its factory defaults.

Syntax

Parameter	Description	Range	Default
`reinit-db`	Reinitializes the WMS database.	—	—

Usage Guidelines

When you use this command, there is no automatic backup of the current database. If an OV-MM server is configured on the WLAN switch (see “mobility-manager” on page 282), this command will fail and return an error.

Example

The following command reinitializes the WMS database:

```
wms reinit-db
WMS Database will be re-initialized. Do you want to proceed with this action [y/n ]:
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable mode on master WLAN switches.

History

This command was available in AOS-W 3.0.

write

```
write {erase [all] | memory | terminal}
```

Description

This command saves the running configuration to memory or displays the running configuration on the screen. This command can also be used to erase the running configuration and return the WLAN switch to factory defaults.

Syntax

Parameter	Description	Range	Default
`erase`	Erases the running system configuration file. Rebooting the WLAN switch resets it to the factory default configuration. If you specify `all`, the configuration and all data in the WLAN switch databases (including the license, WMS, and internal databases) are erased.	—	—
`memory`	Saves the current system configuration to memory. Any configuration changes made during this session will be made permanent.	—	—
`terminal`	Displays the current system configuration.	—	—

Usage Guidelines

Configuration changes made using the CLI affect only the current session. You must save your changes for them to be retained across system reboots. Changes are lost if the system reboots before saving the changes. To save your configuration changes, use the `write memory` command.

If you use the `write erase` command, the license key management database on the WLAN switch is not affected. If you use the `write erase all` command, all databases on the WLAN switch are deleted, including the license key management database. If you reset the WLAN switch to the factory default configuration, perform the Initial Setup as described in the *AOS-W Quick Start Guide*.

If you use the `write terminal` command, all of the commands used to configure the WLAN switch appear on the terminal. If paging is enabled, there is a pause mechanism that stops the output from printing continuously to the terminal. To navigate through the output, use any of the commands displayed at the bottom of the output, as described in Table 5. If paging is disabled, the output prints continuously to the terminal. For more information about the `paging` command, see page 294.

TABLE 5 Output Navigation Keys

Key	Description
q	Exit the display.
u	Page up through the output.
spacebar	Page down through the output.
/	Enter a text string to search for.
n	Repeat the text string to search for.

Example

The following command saves your changes so they are retained after a reboot:

```
write memory
```

The following command deletes the running configuration and databases and returns the WLAN switch to the factory default settings:

```
write erase
```

Platform Availability

This command is available on all platforms.

Licensing Requirements

This command is available in the base operating system.

Command Mode

This command is available in enable and config modes.

History

This command was available in AOS-W 1.0.